Information Security Journal: A Global Perspective

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/uiss20

One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses

Martin Wilson & Sharon McDonald

To cite this article: Martin Wilson & Sharon McDonald (2025) One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses, Information Security Journal: A Global Perspective, 34:1, 15-49, DOI: 10.1080/19393555.2024.2357310

To link to this article: https://doi.org/10.1080/19393555.2024.2357310

© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.

Published online: 31 May 2024.

Submit your article to this journal

Article views: 1124

View related articles

View Crossmark data

Citing articles: 1 View citing articles

Full Terms & Conditions of access and use can be found at https://www.tandfonline.com/action/journalInformation?journalCode=uiss20

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
2025, VOL. 34, NO. 1, 15–49
https://doi.org/10.1080/19393555.2024.2357310

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses

Martin Wilson and Sharon McDonald

School of Design and Informatics, Division of Cybersecurity, Dundee, UK

ABSTRACT

This study examines the cybersecurity needs of UK-based Small and Medium-sized Enterprises (SMEs) via thematic interviews grounded in the Health Belief Model with ten Digitally Dependent SMEs (those who depend on ICT), ten Digitally Based SMEs (those who rely heavily on ICT), and ten Digital Enablers (cybersecurity providers). Previous research highlights SMEs' tendency to underestimate cyber threats, presuming security by obscurity. Our study extends this understanding, revealing SMEs' misjudgment regarding vulnerability to opportunistic attacks due to misunderstanding hackers' indiscriminate methods. Additional findings include SMEs favoring technical solutions over training and policies relying on existing networks and IT suppliers for cybersecurity support. However, c Improving SMEs' engagement with existing cybersecurity advice by enhancing its accessibility is a key area for improvement.

KEYWORDS

Cybersecurity Providers; Digital Enablers; Health Belief Model; Small Business; SME cybersecurity

1. Introduction

Despite the efforts of the UK government policing and other stakeholders (NCSC, 2018), SME cybersecurity adoption remains stubbornly low, as evidenced by UK SMEs' poor cyber essentials uptake (DSIT, 2023). SMEs are major contributors to the economy (Hutton, 2022), making cyber-attacks on them a significant risk to the UK's prosperity. Over a decade of academic research has provided insights into SMEs' perceived barriers to cybersecurity adoption; however, we still know little about how to challenge these barriers and engage with SMEs on their terms. The extant literature tends to treat all SMEs alike, resulting in one-size-fits-all recommendations to improve SME cybersecurity which fails to capture their unique cybersecurity perspectives and engagement preferences (Heidt et al., 2019; Tam et al., 2021; Van Haastrecht et al., 2021). Taking a singular lens to view SME cybersecurity may fail to acknowledge the diverse needs of SMEs, resulting from contextual factors such as resource availability, regulatory awareness, and cybersecurity knowledge. This narrow perspective could result in less effective recommendations for improving SME cybersecurity (Parkin et al., 2016; Shojaifar & Järvinen, 2021). This paper examines SMEs' unique cybersecurity risk perspectives and engagement preferences by conducting qualitative interviews with Digitally Dependent and Digitally Based SMEs. Furthermore, this paper is novel in that it interviewed Digital Enablers to shed light on how to meet heterogeneous SME cybersecurity needs. This study is significant because it enhances the current understanding of countering low SME cybersecurity adoption rates by identifying and characterizing SMEs' heterogeneous cybersecurity needs and engagement preferences. The findings from this study can be utilized by researchers and professionals who collaborate with SMEs to strengthen their cybersecurity measures. By incorporating these insights, they can customize their practices to consider the unique nuances of the SME context. This approach will facilitate the development of more personalized and effective strategies to enhance protective cybersecurity for SMEs. Before describing our primary research, we briefly survey the literature on SME cybersecurity adoption and engagement that has informed our study.

CONTACT Martin Wilson martin.wilson@nebrcentre.co.uk School of Design and Informatics, Division of Cybersecurity, Kydd Building, 40 Bell Street, Dundee DD1 1HG, UK

© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

1.1. SMEs: economic importance, cyber-attacks, cybersecurity, and research

The importance of SMEs to the global economy is widely recognized (Hutton, 2022), with nine out of ten SMEs relying on Information Technology (IT) to conduct their day-to-day business (DSIT, 2023). This reliance was accelerated by the COVID-19 crisis, underscoring the critical role IT plays in the day-to-day business of SMEs (Kergroach & Bianchini, 2021). The 2023 UK Government cybersecurity breaches survey, based on responses from 2,263 businesses, revealed that 32% had fallen victim to cyberattacks, with phishing, e-mail impersonation, and malware being the most common. The survey also unveiled that 32% of micro (1–9 employees) and small businesses (10–49 employees), 59% of medium-sized enterprises (49–249 employees), and 69% of large businesses (250+ employees) encountered at least one cyberattack annually. Moreover, the survey estimated the average cost of an attack at £1,450 for micro and small enterprises, and £4,250 for medium and large companies. Nevertheless, ongoing debates persist regarding the accuracy of these figures. Some researchers argue that attack costs vary significantly depending on the sector (Dieye et al., 2020). In some cases, the full extent of the impacts and costs may not be immediately apparent, such as when depositors relocate wealth holdings from breached banks (Engels et al., 2022). What remains uncontested is the severity of the impacts of such attacks, often leading to SMEs ceasing operations, in stark contrast to their larger counterparts, which possess greater resilience and resources to recover from such incidents (DSIT, 2023; Pagura, 2020).

SMEs can prevent many attacks by taking simple preventative security measures (Such et al., 2015), such as patching, backing up data, and adopting password best practices. These preventative actions are heavily promoted by the UK government, policing, and others (NCSC, 2018, 2020). Yet, SME cybersecurity adoption remains stubbornly low, as evidenced by UK SMEs' poor cyber essentials uptake (DSIT, 2023). Despite the frequency of cyber-attacks, their potentially disastrous impacts, and the UK government's significant investment in cybersecurity, many SMEs still fail to implement adequate security measures. This raises crucial questions about the reasons behind SMEs' cybersecurity reticence and how this issue may be countered through effective engagement strategies.

In recent years, considerable progress has been made in understanding SMEs' cybersecurity needs, and various obstacles to their cybersecurity adoption have been identified. These barriers include inadequate support (Almeida et al., 2018), poor cyber knowledge (Alahmari & Duncan, 2020), lack of resources (Eybers & Mvundla, 2022), discounting vulnerability to cyber-attacks (Wilson et al., 2022), and deprioritization of cybersecurity (Kurpjuhn, 2015). Although the literature on SME cybersecurity engagement preferences is limited, it suggests that SMEs usually search for cybersecurity help and guidance via Google (Renaud & Ophoff, 2021) or their existing technology partners/IT suppliers (Renaud & Weir, 2016). It also appears that SMEs are unaware of the protective guidance provided by the UK government (Wilson et al., 2022). Additionally, being a victim of a cyber-attack is a significant motivator for security adoption (Saban et al., 2021), as is the need to protect brand/reputation (Osborn et al., 2017). Their customers' security expectations also influence SMEs, as does their competitors' security adoption (Barlette et al., 2017), and regulatory compliance is also a driver for adoption (Whitehead, 2020). Despite the significant progress made in understanding the barriers to SME cybersecurity adoption and engagement preferences, recent literature reviews (Heidt et al., 2019; Tam et al., 2021; Van Haastrecht et al., 2021) indicate that most previous research has adopted a one-size-fits-all approach to SME cybersecurity. Therefore, we will now delve into the issues that arise from such approaches.

1.2. SME cybersecurity: a case of one size does not fit all

Existing literature reviews highlight a common tendency among researchers to overlook SMEs' diverse needs and competencies, resulting in generic, one-size-fits-all recommendations (Heidt et al., 2019; Tam et al., 2021; Van Haastrecht et al., 2021). This approach fails to consider contextual factors such as varying resource access, regulatory awareness, and cybersecurity knowledge levels (Alahmari & Duncan, 2020). This leads to

recommendations that may not align with the specific requirements of SMEs and thus yield less effective outcomes (Shojaifar & Järvinen, 2021). For example, to effectively support high-street and online retailers, it's crucial to tailor cybersecurity support to meet the differing needs of such retailers. Drawing from human-computer interaction studies emphasizing diverse user needs, developing SME-centric services requires a deep understanding of user groups (Y. Rogers et al., 2023). By prioritizing this targeted approach, interventions can precisely address the unique requirements of SMEs.

The fact that SMEs are not one homogenous group has necessitated the creation of various classifications that place SMEs into smaller subgroups. These sub-groups differentiate SMEs based on shared characteristics such as location, industry, customer base, turnover, and size (Madani, 2018). However, there is no single, internationally recognized definition of what constitutes an SME, but they are typically categorized based on their workforce size or turnover (Madani, 2018). The benefit of such categorization is that it assists SME research, but crucially, it helps provide tailored support that meets their user needs (Berisha, 2015). Few studies have considered how to categorize SMEs from a cybersecurity perspective, and we now examine emerging work in that field.

1.3. SME heterogenicity: EU's SME digital classification framework

The EU's Small Business Standards Group (SBS) developed a categorization system to provide customized solutions that address SME digital heterogeneity. Their framework identifies three groups: Digital Enablers, Digitally Based, and Digitally Dependent, based on their role and cybersecurity context in the digital ecosystem (SBS, 2020). It also emphasizes the significance of considering SMEs' size and maturity level in conjunction with their digital context, as both factors can impact their cybersecurity practices.

Shojaifar and Järvinen (Shojaifar & Järvinen, 2021) expanded upon the Small Business Standards framework by proposing five distinct SME categories: cybersecurity-abandoned, unskilled, expert-connected, and capable, and cybersecurity provider SMEs. These categories were based on each group's hypothesized levels of cyber policy, knowledge, and relationships. Proposing customized approaches to enhance cybersecurity awareness and competency that align with the differing requirements of each SME group. In their systematic review, Van Haastrecht et al. (Van Haastrecht et al., 2021) examined the socio-technical factors, including goals, people, culture, processes, technology, and assets, to assess their impact on SME cybersecurity. As a result, they recommended that risk assessment methods for SMEs should be tailored to the Small Business Standards categories, with digitally dependent SMEs benefiting from risk assessments that focus on real-world threats rather than hypothetical scenarios. In contrast, digitally based SMEs and digital enablers may require more comprehensive risk assessment methodologies and maturity models that comply with established standards and regulations, as these groups are more likely to follow best practice frameworks and strive to meet compliance requirements.

Although these studies provide helpful recommendations for addressing diverse SME cybersecurity needs, they often lack data collected directly from SMEs to assess the relevance and effectiveness of their models. Furthermore, these studies do not address how to meet the distinct engagement requirements among SME sub-groups. We now focus on one such group, Digital Enablers, who may provide insights into how best to address SMEs' diverse cybersecurity needs and engagement preferences.

1.4. Insights from digital enablers: lessons for SME cybersecurity

Understanding the cybersecurity landscape of SMEs is often challenging due to low engagement rates reported in surveys. Interviews, while based on small samples, offer valuable insights by tapping into the extensive experience of Digital Enablers who have had numerous interactions with this hard-to-reach target audience. By learning from their significant expertise and interactions, researchers can overcome SME engagement's limitations and gain valuable cybersecurity knowledge. However, few researchers have sought to canvas

their views, with work by Wolf et al. (2021), Osborn et al. (2017), Haney and Lutters (2018), and Cartwright et al. (2023) at the literature's forefront.

In their study, Wolf et al. (2021) interviewed nineteen American Chief Information Security Officers (CISOs) with experience working with small businesses. They found that security providers should tailor their cybersecurity guidance to fit the recipients' business context. Similarly, Osborn et al. (2017) conducted twenty interviews with UK SME IT users, cybersecurity providers, and risk holders. Their research revealed that limited resources, knowledge, prioritization of other business processes, reduced system control, and a lack of threat intelligence were some of the factors that prevented SMEs from making effective cybersecurity decisions. They also found that SMEs focused on easy-to-implement cybersecurity technical measures. Haney and Lutters (2018) interviewed twenty-eight cybersecurity advocates from industry, higher education, governments, and not-for-profit organizations. Their research showed that advocates needed to establish trust, impart cyber knowledge, and use various communication and engagement techniques to overcome negative perceptions of cybersecurity. In their study, Cartwright et al. (2023) conducted focus groups and interviews with thirteen UK-based experts in IT and cybersecurity for small businesses. Notably, one prominent theme that emerged was the dual role of IT companies, who can simultaneously contribute to both the solution and the problem in the context of cybersecurity.

There is a clear need for more comprehensive research on SME cybersecurity that includes the views of different stakeholder groups. Only one known study has interviewed representatives from various SME sub-groups, conducted by Osborn et al. (2017). Relying solely on one group's perspective can lead to an incomplete understanding of SME cybersecurity, potentially resulting in unhelpful conclusions. Therefore, it is essential to consider the unique perspectives of different SME subgroups to gain a more comprehensive view of the problem. Furthermore, this study aims beyond merely identifying different perspectives and engagement preferences among heterogeneous SME groups. It seeks to provide practical insights to researchers and professionals working with SMEs, enabling them to improve protective cybersecurity by creating effective strategies for these variations. By interviewing representatives from Digitally Dependent SMEs, Digitally Based SMEs, and Digital Enablers, this study aims to contribute to developing more effective and targeted interventions and engagement practices.

1.5. The present study

This paper analyzes the differing cybersecurity risk perspectives and engagement preferences defined by the Small Business Standards categories of Digitally Dependent SMEs, Digitally Based SMEs, and Digital Enablers. We used data from the thematic analysis of the thirty interviews to conduct a comparative analysis of the three groups.

This was a useful lens through which to frame the following research questions:

RQ1: How do Digitally Dependent and Digitally Based/Digital Enabler groups perceive their/SME vulnerability to cyber-attacks, and what are the mediating factors in their particular contexts?

RQ2: What do Digitally Dependent, Digitally Based, and Digital Enabler groups perceive as effective cybersecurity, and what triggers security adoption?

RQ3: What are the Digitally Dependent, Digitally Based groups' cybersecurity engagement practices, and what engagement tactics does the Digital Enabler group use to persuade SMEs to adopt protective security?

The results of this analysis will help those who work with SMEs to improve cybersecurity by helping them meet diverse SME cybersecurity needs.

2. Materials and methods

This section describes the research design, data collection, and data handling.

2.1. Participants

This study involved thirty participants, with ten individuals in each category, as shown in Table 1.

Table 1. Digitally Dependent, Digitally Based, and Digital Enabler group classifications used in this study.

Group Name	Description
Digitally Dependent	SMEs whose use of software and IT, are secondary to their main business focus, e.g., they do not sell software or online services. However, they depend on IT and software to run their day-to-day business.
Digitally Based	SMEs whose use of software and IT formed part of their main business offering, e.g., they sell or develop software or operate via software, e.g., providing online services for other businesses to use. Crucially they did not offer cyber, or IT support to other businesses.
Digital Enablers	Business-to-business cybersecurity consultants whose main commercial aim is to help other businesses become more cyber secure

Interview recruitment was facilitated through the first author's connections within the National CRC Group (2023). The CRC network consists of not-for-profit centers that bring together academia, law enforcement, and private-sector businesses to assist SMEs in adopting cybersecurity. A purposive sampling method (Bernard, 2017) was employed to select participants who met the Digitally Dependent and Digitally Based SMEs criteria. To identify suitable interviewees, prospective individuals in these categories completed a brief online screening survey, providing details regarding their business demographics and IT usage. Furthermore, Digital Enablers were recruited from the Northeastern CRC's cyber expert panel. Thirty interviews were conducted, with ten participants each from the Digitally Dependent, Digitally Based, and Digital Enabler categories.

2.2. Question design

Semi-structured interviews were chosen, and the question design used a generative approach (utilizing open-ended and exploratory questions that encouraged interviewees to provide detailed and nuanced answers) to gain a deep understanding of SMEs' cybersecurity motivations, pain points and behaviors to understand better why SMEs fail to adopt protective security.

2.3. Conceptual framework used to ground questions

To establish a theoretical backdrop, models from public health were used, as it has been proven that interventions designed to promote the adoption of preventative healthcare behaviors are more successful when based on established theories (Tebb et al., 2016). Preventative healthcare encompasses behaviors that contribute to a healthy lifestyle and minimize the impact of poor health. Similarly, protective cybersecurity countermeasures share similarities with preventative healthcare, as both involve implementing preventive actions to avoid undesirable outcomes. However, it should be noted that protective cybersecurity measures require ongoing persistence due to the ever-evolving nature of the cyber threat landscape. Protection Motivation Theory (R. W. Rogers, 1975) and Health Belief Model (Abraham & Sheeran, 2015) are two health models at the forefront of cybersecurity research. Comparing the two models for suitability to be applied to this study, the Health Belief Model has an additional construct of cues to action, which may reveal valuable insights into what triggers SME cybersecurity adoption. Therefore, it was used as a theory to ground developed interview questions, as shown in Table 2.

Developed questions were piloted with cybersecurity professionals, SME owners, and academics to ensure questions were technically correct, free from bias, avoided repetition, and unambiguous. Discussions were focused on a baseline comparison of primary topics among interviewees. Sub-questions related to different aspects of central topics while allowing flexibility to probe with additional questions when interesting and unexpected themes emerged. Interviews were conducted using a laddering technique, where authors probed seemingly simple responses to questions to identify underlying motives (Reynolds & Gutman, 1988).

2.4. Conducting interviews

Video conferencing software was used to conduct this research. No incentives were offered to take part in the interviews. The first author conducting the interviews was an experienced and accredited UK police detective who has conducted thousands of victim and suspect interviews over 20 years. The author used this experience to put participants at ease and obtain the best possible accounts.

Table 2. Interview themes and question areas DD = Digitally Dependent, DB = Digitally Based, DE = Digital Enabler.

Group	HBM Construct/Question Area	Question areas or probe motivations	Source/Adapted From
DD, DB & DE	HBM – Perceived Vulnerability	How vulnerable do you believe your business/SMEs are to cyber-attack? Which types of attacks are more or less likely? Do you think cybercrime is more of an issue for larger organizations, or are SMEs just as vulnerable? Do you know of any businesses which have been subjected to a cyber-attack? How might your business/SMEs be hacked?	Claar (2011)
DE	HBM – Perceived Vulnerability	In your experience, do SMEs deliberately leave themselves vulnerable? In your experience do SMEs have an accurate appraisal of their cyber risks?	Self-Developed
DD & DB	HBM – Perceived Vulnerability	What do you understand by the term hacking? How visible is your business to a hacker?	Self-Developed
DD & DB	HBM – Perceived Severity	How might your business/SMEs be hacked? What might the impacts be?	Claar (2011)
DD, DB & DE	HBM – Perceived Benefits	What do you see/SMEs see as the return on any investment in cybersecurity? What positives come from investment?	Ng et al. (2009)
DD, DB & DE	HBM- Perceived Barriers	What stops you/SMEs from investing in cybersecurity? What do you think the biggest barriers are to SME cybersecurity adoption?	Ng et al. (2009)
DD, DB & DE	HBM- Self-Efficacy	How do you/SMEs maintain cybersecurity? Do you/SMEs have any issues implementing cybersecurity?	Ng et al. (2009)
DD, DB & DE	HBM - Cues to Action	What motivates you/SMEs to adopt cybersecurity?	Self-Developed
DE	Engagement	With regards to cybersecurity, what do SMEs ask you for help with? How do you contact SMEs in order to speak to them about cybersecurity? What works best when persuading them that cybersecurity is important and worth investing in?	Self-Developed
DD & DB	Engagement	Have you heard of the National Cybersecurity Centre (NCSC)? How do you currently receive cybersecurity guidance? How would you like to receive cybersecurity guidance?	Self-Developed
DD, DB & DE	Cues to action	What triggers cybersecurity adoption within your business/SMEs? What makes you/SMEs keep security up to date?	Self-Developed
DD & DB	Influencers	Considering cyber-attacks upon businesses which are reported in the news, what influence do they have on your security adoption? In what ways, if any, are these news stories like your business context? Do these news stories scare you in any way?	Self-Developed
DD, DB & DE	Improvements	What can be done to improve the future of SME cybersecurity?	Self-Developed

Interviews averaged 20 minutes and had the following stages:

(i) Ice breaking and building rapport – interviewees were put at ease by introducing and conversing politely.
(ii) Main questions – The interview protocol gave structure; however, interviewees were allowed to stray into other areas, and the interviewer was agile enough to adapt and maintain a conversational style.
(iii) Wrap up – next steps and opportunity for the interviewee to ask questions.

2.5. Transcription

Video conferencing software facilitated the initial recording and automatic transcription of research interviews, serving as preliminary drafts. The first author meticulously verified these transcriptions by immersing in the audio recordings, cross-referencing them with the automated transcripts, and making necessary corrections to ensure accuracy. The goal was to achieve verbatim transcripts capturing the context precisely. This rigorous process enhanced the author's familiarity with the data, aligning with Strauss and Corbin (1998) recommendations. To safeguard anonymity, identifiers were removed, and interviewees were assigned pseudonyms (DD, DB, DE) along with numbers 1–10.

2.6. Data analysis, reliability, and reduction

Figure 1 shows the themes and sub-themes identified from interview transcripts. The following section discusses the thematic coding process, the intercoder reliability coefficient calculation, data reduction strategies, theme/sub-theme identification, and analysis.

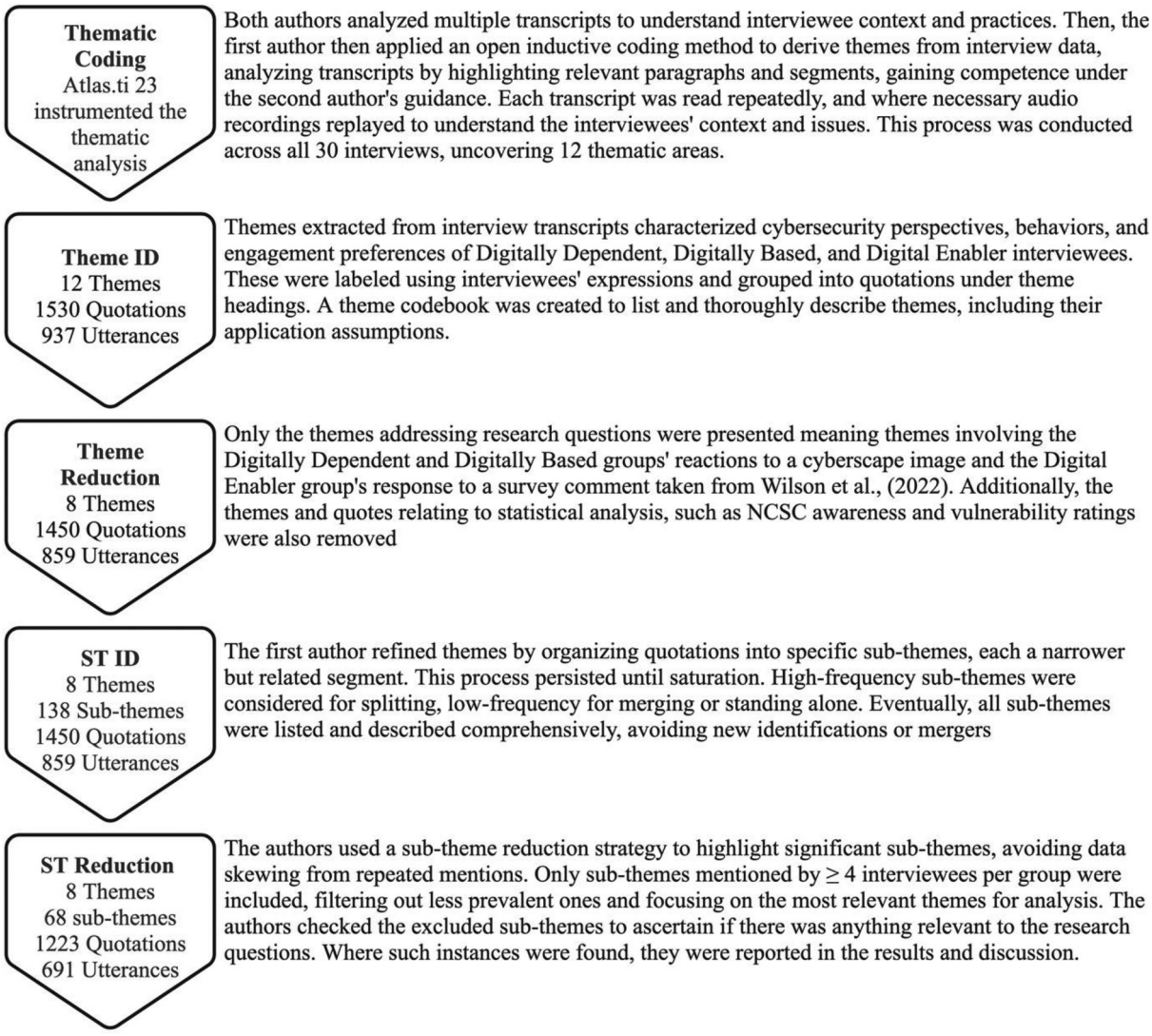

Figure 1. illustrates identifying themes and sub-themes from interview transcripts, identifying significant sub-themes while excluding less relevant ones from the analysis (ST = sub-theme, ID = identification).

2.7. Intercoder reliability (ICR)

Intercoder reliability (ICR) assesses consistency in data interpretation by having a secondary coder independently code interview data. The authors ensured ICR by having a secondary coder code at least 25% of the interviews at the theme level. Using a predefined theme code book, the second author applied themes to nine random interview transcripts received in an Atlas.ti 23 project. Subsequently, an inter-rater reliability procedure indicated reliable results (Krippendorff's alpha value $\alpha = 0.73$) (Friese, 2019).

3. Results

Here we present our results. First, we consider the participant demographics and their answers to a screening survey about current IT use within their business. Then, we present our qualitative analysis by theme and sub-theme level.

3.1. Respondent characteristics

Table 3 presents the interviewee demographic characteristics obtained from a short pre-interview survey.

3.2. The reported IT use by our digitally dependent and digitally based groups

Table 4 displays the management of IT, current practices, data types processed, and past victimization among the Digitally Based and Digitally Dependent Groups.

Table 3: Digitally Dependent, Digitally Based, and Digital Enabler group sample characteristics

Demographic Factor	Digitally Dependent	Digitally Based	Digital Enablers
Number	n = 10	n = 10	n = 10
Company Size	Micro n = 10	Micro n = 8 Small n = 2	N/A
Respondent's Position	Owner/partner n = 7 Management n = 3	Owner/partner n = 10	Owner/partner n = 7 Management n = 3
Region	NE & Yorkshire n = 9 East Midlands n = 1	NE & Yorkshire n = 9 Southwest n = 1	NE & Yorkshire n = 10
Business Sector	Food and Hospitality = 1 Media n = 2 Charity n = 2 Retail or wholesalen = 2 Events n = 1 Consultancy n = 1 Construction n = 1	Retail or wholesalen = 1 Recruitmentn = 2 Software developmentn = 6 Social Median = 1	Cybersecurity consultancy n = 10
Business Age	Mean = 9.1 years Mode = 1 year Median = 4.5 years Range = 45 years	Mean = 11.5 years Mode = N/A Median = 8 years Range = 43 years	N/A
Number of SMEs DEs worked with to improve security	N/A	N/A	Mean = 862 Mode = 150 Median = 175 Range = 4,890

Table 4. Digitally dependent and digitally based respondents self-reported it practices.

IT Practices	Digitally Dependent	Digitally Based
Number	n = 10	n = 10
How IT is managed	DIY *n* = 6	DIY *n* = 1
	In-house team member *n* = 1	In-house team member *n* = 4
	Outsourced *n* = 3	In-house IT Personnel *n* = 1
		Outsourced *n* = 4
Mean no of devices	8.2	14.8
Median no of devices	4.5	10
Mode no of devices	2	6
Range no of devices	23	45
Standardized IT procurement*	No *n* = 10	No *n* = 10
Logging	No *n* = 10	No *n* = 8
		Yes *n* = 2
IT dependency	High *n* = 9	High *n* = 10
	Somewhat *n* = 1	
Online Banking	Yes *n* = 10	Yes *n* = 10
PII	Yes *n* = 6	Yes *n* = 8
	No *n* = 4	No *n* = 2
Pay online	Yes *n* = 6	Yes *n* = 4
	No *n* = 4	No *n* = 6
Victim	Yes *n* = 1	Yes *n* = 2
	No *n* = 9	No *n* = 8

3.3. Reported defensive actions taken

Figure 2 shows the results from the pre-interview screening survey which asked Digitally Dependent and Digitally Based groups to select what cybersecurity defensive actions they had taken from a range of options.

The defensive actions data were aggregated into the three ISO pillars of People, Processes and Technology Pillars (Schneier, 2009) as follows:

People (Training) Processes (CE, ISO27001, Vulnerability Assessment, Pen Test, Backup) Technology (Firewall, Antivirus, 2FA, IDS, Encryption, other (password manager)).

Figure 3 shows the results of this aggregation and an over-reliance on technical security measures can be observed.

3.4. Vulnerability ratings

When Digitally Dependent (DD) and Digitally Based interviewees (DB) were asked how vulnerable their business was to a cyber-attack, or in the case of Digital Enablers (DE), how vulnerable SMEs were to attack, interviewees responses were categorized as follows:

(1) = Don't Know
(2) = Low
(3) = Average
(4) = High

The mean vulnerability rating for DD = 2.1, DB = 2.7, and DE = 4.

A Kruskal-Wallis test showed significant differences between the perceived vulnerability ratings of

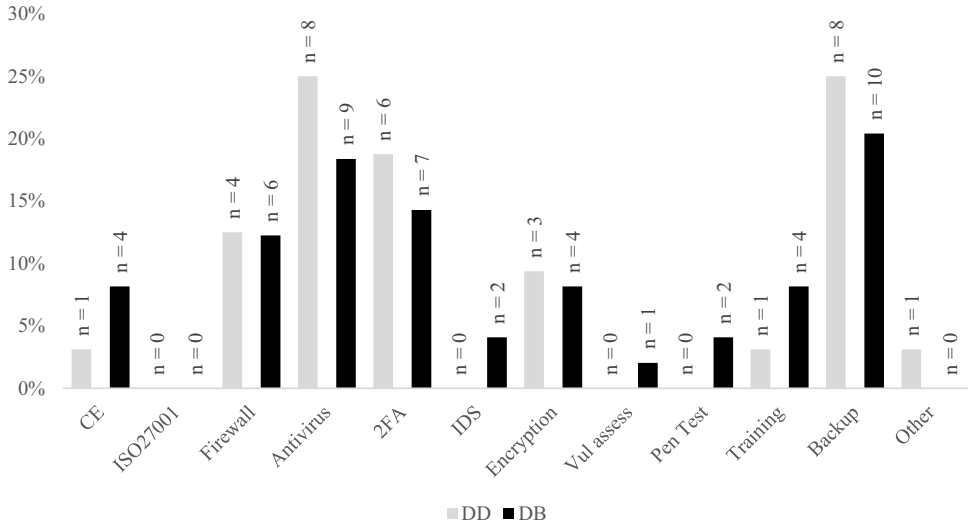

Figure 2. Online screening survey results - defensive actions taken by Digitally Dependent and Digitally Based groups with counts and percentages (Other = password manager).

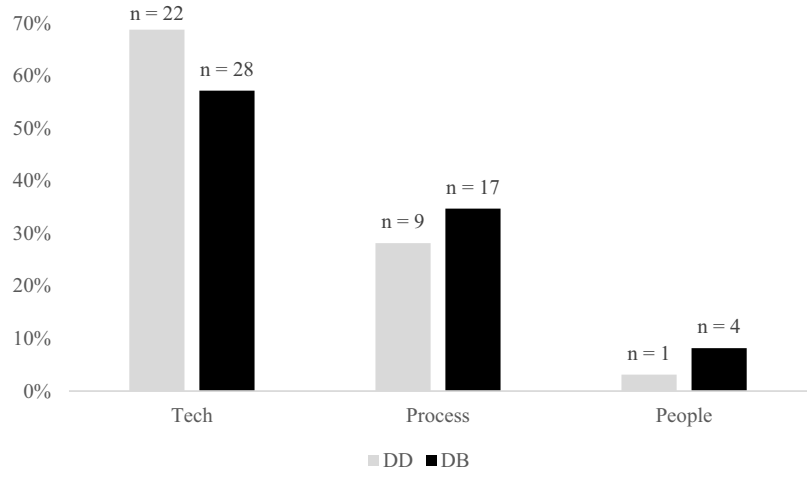

Figure 3. Online screening survey results - defensive actions taken by Digitally. Dependent and Digitally Based groups with counts and percentages.

our groups $H(2) = 16.637$, $p < .001$. A Mann-Whitney U test between groups revealed significant differences as shown in Table 5.

3.5. National Cybersecurity Centre (NCSC) awareness

Digitally Dependent and Digitally Based interviewees were asked if they had heard of the National Cybersecurity Centre (NCSC), with 70% ($n = 7$) of Digitally Based group interviewees knowing of the NCSC compared to only 30% ($n = 3$) of the Digitally Dependent group.

3.6. Thematic analysis

We present data from our qualitative analysis at the theme level, followed by sub-theme level analysis. Readers will note that the themes/sub-themes are presented in tabular format arranged by descending interviewee count (IC). Table 6 explains how we present the findings of our thematic analysis, focusing on the theme level. In Table 7, we elaborate on how we present the results of our sub-theme analysis.

Table 8 shows the group theme analysis.

Table 5. Perceived vulnerability rating results of Mann-Whitney U test conducted between groups, with corresponding effect sizes.

	Digitally Dependent	Digitally Based	Digital Enablers
Digitally Dependent			
Digitally Based	U = 66.5, d = 0.97		
Digital Enablers	*U = 93.0, d = 0.81	*U = 87.5, d = 0.62	

**Significant difference obtained at p < .05.*
Effect size (d) benchmarks suggested by Cohen, (1988) refer to effect sizes as small (d = 0.2), medium (d = 0.5), and large (d = 0.8).

Table 6. Example table demonstrating how theme data is presented.

Theme	Description	Group	TC	IC	F
Name of theme	Written description of theme	All	Cumulative count of all groups	Cumulative count of all groups	Cumulative frequency of all groups as a %
		DD	Individual count	Individual count	Individual %
		DB	Individual count	Individual count	Individual %
		DE	Individual count	Individual count	Individual %

TC = Theme count, the number of times interviewees uttered a quote that fitted a theme.
IC = Interviewee count, the number of times interviewees mentioned a theme.
F = (Theme Rel Frequency = Theme count/Total number of all theme quotations) x 100.
All = Digitally Dependent + Digitally Based + Digital Enablers.
DD = Digitally Dependent.
DB = Digitally Based.
DE = Digital Enabler.

Table 7. Example table demonstrating how sub-theme data is presented.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Name of sub-theme	Written description of sub-theme	*Quotation uttered by interviewee which is representative of the sub-theme, followed by anonymised identifier in brackets*	All	Cumulative count of all groups	Cumulative count of all groups	Cumulative frequency of all groups as a %
			DD	Individual count	Individual count	Individual %
			DB	Individual count	Individual count	Individual %
			DE	Individual count	Individual count	Individual %

STC = Sub-theme count, the number of times interviewees uttered a quote that fitted the sub-theme.
IC = Interviewee count, the number of times interviewees mentioned a sub-theme.
TF = (Theme Rel Frequency = Sub-theme count/Total number of that theme's quotations) x 100.
All = Digitally Dependent + Digitally Based + Digital Enablers.
DD = Digitally Dependent.
DB = Digitally Based.
DE = Digital Enabler.

The interviewees had lots to say about risk, with nearly half of all quotations residing in the risk perceptions factor theme. Few Digitally Dependent interviewees uttered quotations that fit the cue-to-action theme; this will be discussed in more detail at the sub-theme level.

Table 9 shows the analysis of threat knowledge sub-themes within the risk perception factors theme.

3.7. The influence of threat knowledge upon risk perceptions

When assessing the effect of cyber threat knowledge on risk perceptions, it was clear that such knowledge was a moderating factor. There was unanimous agreement across all interviewee groups that SMEs don't grasp threats, e.g., *"I've got only very minimal knowledge about the different techniques that they use for doing it" (DB9)*. There was further evidence of this lack of threat knowledge when our Digitally Dependent and Digitally Based interviewees were asked to describe how they thought their business might be attacked, with three-quarters of them giving poor attack descriptions, e.g., *"Somebody getting onto your system" (DD3)*. Digital Enablers exclusively felt

Table 8. Group theme analysis.

Theme	Description	Group	TC	IC	F
Risk Perception Factors	What factors affect Digitally Dependent and Digitally Based groups perception of their business's cyber risk? Or in the case of Digital Enablers, factors which they believe are influencing SMEs risk judgments?	All	601	337	49.1%
		DD	202	112	16.5%
		DB	178	105	14.6%
		DE	221	120	18.1%
Engagement	How do Digitally Dependent and Digitally Based groups get cybersecurity guidance, and who assists them? How do Digital Enablers approach SMEs about cybersecurity, and what prompts SMEs to seek their help? What are Digital Enablers' views on cybersecurity guidance?	All	123	85	10.1%
		DD	34	27	2.8%
		DB	51	34	4.2%
		DE	38	24	3.1%
Improvements	Suggestions to improve the future of SME cybersecurity engagement/adoption	All	83	52	6.8%
		DD	21	15	1.7%
		DB	26	16	2.1%
		DE	35	20	2.9%
Cues to Action	Triggers for SME cybersecurity adoption	All	108	53	8.8%
		DD	7	5	0.6%
		DB	22	14	1.8%
		DE	79	34	6.5%
Engagement Tactics*	Effective tactics used to persuade SMEs into adopting cybersecurity. Includes ineffective tactics	DE	137	55	11.2%
News**	Views on business cybersecurity media reporting	DD & DB	81	49	6.6%
		DD	33	24	2.7%
		DB	48	25	3.9%
Return on investment (ROI)	Views on the value of cybersecurity/return on investment	All	74	44	6.1%
		DD	21	13	1.7%
		DB	37	22	3.0%
		DE	16	9	1.3%
Cyber Criminal Perceptions**	Interviewees perceptions of a hacker e.g. characteristics, demographics	DD & DB	16	16	1.3%
		DD	7	7	0.6%
		DB	9	9	0.7%

*A Digital Enabler group exclusive theme.
**A Digitally Based and Digitally Dependent group exclusive theme.

that the intangible nature of threats made them more challenging to comprehend for small businesses, e.g., *"I mean it's intangible because he or she can't see it or feel it" (DE9).*

3.8. Threat misconceptions – security in obscurity

Compounding matters were two threat knowledge misconceptions that SMEs were too small to be attacked, e.g., *"Why would anyone go after me? It's literally me and my laptop" (DD3)*. The second misconception was SMEs who believed they had nothing worth stealing, e.g., *"I don't think we have much that anybody wants" (DB5)*. These misconceptions may be why some SMEs believe they don't need to implement protective security, as they believe they have security in obscurity.

3.9. Understanding hacker motivations

If attacks were to happen, there was a consensus across all groups that hackers were motivated to steal data. Digitally Dependent interviewees exclusively believed criminals wanted to steal personally identifiable information (PII), e.g., *"Using your name and your identity for fraudulent purposes" (DD3)*, and criminals wanted to steal bank details, e.g., *"The concern would be them going after our bank details" (DD6).*

3.10. Interviewee's knowledge of business victims of cyber-attacks

Unsurprisingly, all our Digital Enablers knew victims, as their clients often approached them asking for help recovering from attacks, e.g., *"We see a lot of victims on zone H" (DE2)*. Fewer Digitally Dependent and Digitally Based SMEs reported being a victim of knowing of victims in their interviews.

Table 9. Analysis of threat knowledge sub-themes within the risk perception factors theme.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Don't grasp threats	Poor cyber threat knowledge	*Awareness of threats (DE5)*	All	48	21	8.0%
			DD	23	8	3.8%
			DB	11	6	1.8%
			DE	14	7	2.3%
Knows victims	Reports being a cyber victim, or personally knows other businesses victims	*We've already had our website hacked (DD9)*	All	22	21	3.7%
			DD	5	5	0.8%
			DB	7	6	1.2%
			DE	10	10	1.7%
Criminals want data	Interviewees report that attackers want to steal data	*Stealing data (DB6)*	All	19	16	3.2%
			DD	6	5	1.0%
			DB	8	6	1.3%
			DE	5	5	0.8%
Nothing worth stealing	SMEs believe their business has nothing of value to potential attackers	*I'm not important, what do I have? (DD6)*	All	28	15	4.7%
			DD	17	8	2.8%
			DB	7	5	1.2%
			DE	4	2	0.7%
Poor attack description**	Interviewee gives poor description of how attacks occur	*Somebody else trying to gain access to your computer (DD6)*	DD & DB	18	15	3.0%
			DD	10	9	1.7%
			DB	8	6	1.3%
Too small to be attacked	SMEs believe that their business is too small to be of interest to attackers	*It's literally me and my laptop (DD3)*	All	16	8	2.7%
			DD	9	4	1.5%
			DB	2	2	0.3%
			DE	5	2	0.8%
Intangible nature of threats	Intangible nature of cyber threats, makes them difficult to comprehend	*Cyber is quite etheral until you've been hit (DE10)*	All	8	5	1.3%
			DD	0	0	0.0%
			DB	0	0	0.0%
			DE	8	5	1.3%
Criminals want bank details	Interviewee reports that attackers want to steal bank details	*The concern would be bank details (DD3)*	All	8	5	1.3%
			DD	8	5	1.3%
			DB	0	0	0.0%
			DE	0	0	0.0%
Criminals want PII	Interviewees state that attackers want to steal personally identifiable information	*Take your identity for fraudulent purposes (DD5)*	All	5	5	0.8%
			DD	5	5	0.8%
			DB	0	0	0.0%
			DE	0	0	0.0%

**A Digitally Based and Digitally Dependent group exclusive theme.

Table 10 shows the analysis of risk judgment sub-themes within the risk perception factors theme.

3.11. Group disagreement about the level of risk posed by opportunistic cyber-attacks

All groups had different opinions on which attack category was most risky to their business. Namely, the sub-themes risk from targeted attacks and risk from untargeted attacks. All Digital Enablers thought that SMEs were extremely vulnerable to opportunistic, untargeted attacks, e.g., "*Targeted attacks only happen for very large enterprises, you know state-sponsored, hacktivism, these attacks are absolutely never going to touch SMEs. But the fact is their real danger lies in all the commodity-based stuff that's out there. You know the clickbait, it's not targeted. It's fire as much out there as possible and waits for somebody to click it (DE6)*. Conversely, Digitally Dependent and Digitally Based groups felt the greater risk came from targeted attacks, e.g., "*I think the bigger threat comes from targeted attacks" (DB4)*. One Digital Enabler mentioned the targeted attack sub-theme. The disparity could be rooted in a lack of threat knowledge. This was the conclusion of our Digital Enablers,

Table 10. Analysis of risk judgment sub-themes within the risk perception factors theme.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Risk form untargeted attacks	Interviewee perceives risk from attacks which indiscriminately target as many victims as possible	*SME breaches that I have investigated have been primarily through automated style of attacks which just propagating across the Internet based on IP address (DE2)*	All	40	18	6.7%
			DD	2	2	0.3%
			DB	15	6	2.5%
			DE	23	10	3.8%
Risk from phishing	Interviewee perceives risk from phishing attacks	*Email threats (DE1)*	All	38	18	6.3%
			DD	11	5	1.8%
			DB	16	7	2.7%
			DE	11	6	1.8%
Impacts are severe	Cyber attacks can cause major business impacts	*The implications could be so damaging (DB3)*	All	22	15	3.7%
			DD	11	7	1.8%
			DB	5	4	0.8%
			DE	6	4	1.0%
Risk form targeted attacks	Interviewee perceives risk from perpetrators who deliberately target specific organisations	*There's a targeted element where they to make statements (DB6)*	All	18	13	3.0%
			DD	9	5	1.5%
			DB	8	7	1.3%
			DE	1	1	0.2%
Risk form website attacks	Increased risk from website attacks	*Web apps (DE8)*	All	14	10	2.3%
			DD	4	4	0.7%
			DB	6	4	1.0%
			DE	4	2	0.7%
Can't assess risk	SMEs can't or haven't made accurate risk jugements	*I think a lot of people don't quantify that risk (DE10)*	All	8	6	1.3%
			DD	0	0	0.0%
			DB	0	0	0.0%
			DE	8	6	1.3%

who painted a picture that SMEs can't accurately assess risk, e.g., *"I don't think they have got a true accurate appraisal" (DE3).*

3.12. Attacks and impacts

All groups agreed that the impacts of attacks could be severe, e.g., *"I mean, it can cripple an organization" (DB7)*. All groups felt phishing represented a major risk to SMEs, *"Probably a phishing attack, someone sending us an email link, and us clicking through, putting the password in" (DB2)*. There was broad agreement that there were risks from website attacks, e.g., *"My website" (DD3), "Exploiting a weakness on the website" (DB8).*

Table 11 shows the analysis of protective cybersecurity sub-themes within the risk perception factors theme.

3.13. A protective cybersecurity knowledge vacuum

All groups agreed that SMEs struggle to grasp security, e.g., *"I'm nowhere near knowledgeable enough about it at the moment" (DB1)*. Digital Enablers said that SMEs didn't grasp security processes, e.g., *"When did you last test your disaster recovery procedures? Or take your backup and restore your backup, and see exactly what state the data is in?" (DE3)*. The lack of protective security knowledge manifested itself across other sub-themes, with Digital Enablers complaining that SMEs were too tech-centric in their approach to security. As one Digital Enabler put it, *"I don't really think they take the right approach, I think they are just seeing everything as, oh yeah, we'll fix that problem by buying a product, but it's not really just about products" (DE1)*. When we asked the Digitally Dependent and Digitally Based groups what security measures they had taken, thirteen interviewees described deploying technical security measures, e.g., *"Anti-virus" (DD8)*. Eleven described deploying security processes, e.g., *"Offsite backups" (DB6)*. Noticeable by its absence was the People sub-theme, which did not have sufficient interviewee counts (IC) to meet our inclusion criteria, e.g., "*We train our staff on how to handle data" (DB3)*. Digitally Dependent and Digitally Based groups do

Table 11. Analysis of protective cybersecurity sub-themes within the risk perception factors theme.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Don't grasp security	SMEs vulnerability is linked to the level of cyber understanding	*I do think the problem is just understanding it (DB4)*	All	53	24	8.8%
			DD	21	8	3.5%
			DB	17	8	2.8%
			DE	15	8	2.5%
Deployed tech Security**	Interviewee describes protective technology deployed	*We have antivirus (DB3)*	DD & DB	36	13	6.0%
			DD	19	6	3.2%
			DB	17	7	2.8%
Deployed security Processes**	Interviewee describes protective processes implemented	*I have backed everything up (DD3)*	DD & DB	22	11	3.7%
			DD	5	4	0.8%
			DB	17	7	2.8%
Other functions prioritized	Other more pressing business priorities are prioitised ahead of/at the expense of cybersecurity	*We've got other priorities, basically, which don't allow me to to look at that just now (DD9)*	All	12	10	2.0%
			DD	3	3	0.5%
			DB	5	3	0.8%
			DE	4	4	0.7%
Are too tech centric	SMEs think of cybersecurity purely in technical/ deployment of protective tool terms	*Their reliance is very much on AV, that is their predominantly only line of defence (DE5)*	All	13	9	2.2%
			DD	0	0	0.0%
			DB	2	2	0.3%
			DE	11	7	1.8%
Don't grasp processes	SMEs vulnerability is linked to the level of cyber process understanding	*There is very little in the way of detection and response capabilities (DE1)*	All	13	8	2.2%
			DD	0	0	0.0%
			DB	1	1	0.2%
			DE	12	7	2.0%

**A Digitally Based and Digitally Dependent group exclusive theme.

not seem to appreciate the defensive value of cybersecurity training for themselves or their employees.

3.14. Other business functions are prioritized ahead of cybersecurity

Combing a lack of threat knowledge, protective security understanding, and ability to accurately judge risk probably results in other business functions being prioritized ahead of cybersecurity, e.g., *"It's not at the front of my mind as I'm concentrating on what we do best" (DD10).*

Table 12 shows the analysis of the influence of SME IT suppliers and the cybersecurity sector subthemes on risk perceptions within the risk perception factors theme.

3.15. SME IT suppliers

Digitally Dependent and Digitally Based groups believed their IT/managed service Digital Enablers kept them safe. Digital Enablers said that SMEs assumed this was the case, e.g., *"I rely on our IT providers looking after us" (DD2)*. Digital Enablers described how this belief appeared routed in "presumption" and "hope" rather than knowing what their suppliers did or understanding their service level agreements (SLA). Concerningly, Digital Enablers exclusively felt that some IT suppliers were inept regarding cybersecurity, e.g., *"There are a lot of small IT companies that have turned their hand to security and are selling its wares, but effectively all they do is just install AV" (DE5)*. This could leave many SMEs exposed, thinking their IT supplier has them covered when they don't or can't protect them.

3.16. Perceptions that the cyber sector is only interested in selling products

Half of our interviewees complained that the cybersecurity sector was too sales driven and that such practices were degrading trust and potentially increasing vulnerability, e.g., *"Getting ripped off by somebody trying to pretend that I need XY and Z when I only really need Z (DD4)*. Alarmingly, Digital Enablers expressed concern that the cyber sector was misleading SMEs into a false sense of security, e.g., *"The little snake oil sellers, as we*

Table 12. Analysis of the influence of SME it suppliers and the cybersecurity sector sub-themes on risk perceptions within the risk perception factors theme.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Sector is sales driven	Security sector sell its products, irrespective of whether or not those products are suitable for clients	*The market is designed to sell things, not necessarily fix problems (DE7)*	All	27	15	4.5%
			DD	6	4	1.0%
			DB	6	4	1.0%
			DE	15	7	2.5%
IT keeps me safe	Reply on existing IT supplier/managed service provider to keep them safe	*I rely on XXXX protecting all of that data (DD8)*	All	17	10	2.8%
			DD	13	6	2.2%
			DB	4	4	0.7%
			DE	0	0	0.0%
Sector Misleads	SMEs are deceived into believing they are safe as a result of promises made by the security sector	*Misleading information from vendors (DE2)*	All	19	6	3.2%
			DD	0	0	0.0%
			DB	0	0	0.0%
			DE	19	6	3.2%
Inept IT	IT providers are not competent to do cybersecurity	*A lot of IT providers don't understand it (DE1)*	All	10	5	1.7%
			DD	0	0	0.0%
			DB	0	0	0.0%
			DE	10	5	1.7%

Table 13. Analysis of resource barriers sub-themes within the risk perception factors theme.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Lack money	SMEs don't have the money to implement cybersecurity	*Cost (DE4)*	All	36	17	6.0%
			DD	4	3	0.7%
			DB	10	5	1.7%
			DE	22	9	3.7%
Lack time	SMEs don't have time to implement cybersecurity	*It boils down to time (DD5)*	All	20	9	3.3%
			DD	9	4	1.5%
			DB	3	2	0.5%
			DE	8	3	1.3%
Lack access to expertise	SMEs lack access to cyber expertise	*We don't have anybody in house sadly (DD9)*	All	11	9	1.8%
			DD	2	2	0.3%
			DB	3	3	0.5%
			DE	6	4	1.0%

crudely call them, you know the little widget, people buy this, and you will be safe forever girls and boys, sad, isn't it?" (DE9). The fact that this sub-theme was not mentioned by any Digitally Dependent or Digitally Based interviewees suggests that they were unaware of such misleading behavior.

Table 13 shows the analysis of resource barriers sub-themes within the risk perception factors theme.

3.17. Not enough money, time, and a lack of access to expertise

When it came to a lack of resources that were influencing SME vulnerability to cyber-attacks, the sub-theme lack of money was mentioned chiefly by Digital Enabler and Digitally Based groups; only two Digitally Dependent interviewees felt that money was a barrier to cybersecurity, which suggests that the more tech-centric a business becomes, the greater the perceived financial costs are to defend it, e.g., *"The cost" (DD9)*. There was agreement across all groups that a lack of time, e.g., ", *"I just don't have the time" (DB3)*, and a lack of access to expertise, e.g., *"Not everyone has IT support" (DD7)*, were barriers to cybersecurity.

Table 14 shows the analysis of Digitally Dependent and Digitally Based cybercriminal perception's sub-themes.

3.18. Hacker perceptions of the digitally dependent and digitally based group

Both Digitally Dependent and Digitally Based groups perceived hackers to be the stereotypical hooded

Table 14. Analysis of Digitally Dependent and Digitally Based cybercriminal perception's sub-themes.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Criminals are hoodies**	Interviewee describes a cyber criminal as the stereotypical teenager wearing a hoodie in a bedroom, with limited social skills	*The stereotype, IT geek sat behind the screen (DD3)*	DD & DB	10	10	62.5%
			DD & DB	5	5	31.3%
			DB	5	5	31.3%
Criminals are organized**	Interviewees believe that hacking is linked to organized crime	*Organised crime (DD10)*	DD & DB	6	6	37.5%
			DD & DB	2	2	12.5%
			DB	4	4	25.0%

**Exclusive Digitally Dependent and Digitally Based sub-theme.

Table 15. Analysis of news sub-themes.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Big business attacks**	When asked to recall cyber-attacks upon businesses reported in the media, the interviewee only describes big business attacks	*Large PLCs have been hacked (DD3)*	DD & DB	35	19	43.2%
			DD	14	9	17.3%
			DB	21	10	25.9%
News reports irrelevant**	Interviewee believes that media reporting of attacks upon business isn't relevant to their business context	*If a news article came out today I wouldn't be thinking oh Jesus we better do something about that (DB7)*	DD & DB	30	17	37.0%
			DD	13	9	16.0%
			DB	17	8	21.0%
Cautious after news**	Interviewee says that media reporting of cyber-attacks upon business illicits checking and caution	*They concern me (DB5)*	DD & DB	16	13	19.8%
			DD	6	6	7.4%
			DB	10	7	12.3%

**Exclusive Digitally Dependent and Digitally Based sub-theme.

teenager sitting in a bedroom, e.g., *"The only image I can conjure up is a guy in a dark bedroom with pot, noodles everywhere, and it's late at night" (DD1)*. This stereotype is probably media generated, as most media reporting and even promoting cybersecurity products invariably uses the imagery of a hooded cybercriminal sitting behind a computer screen. The problem is that such stereotypical images do not represent the threat landscape, and their use could reinforce vulnerability misconceptions. More representative of the actual threat landscape is the industrialization of cybercrime (Microsoft, 2022), where perpetrators are organized criminals, e.g., *"It's probably more criminal gangs" (DB2).*

Table 15 shows the analysis of news sub-themes.

3.19. Media reporting of cyber-attacks upon business were perceived to be irrelevant

Overall, our Digitally Dependent and Digitally Based groups paid little attention to business cyber-attacks reported in the media, feeling that they were irrelevant to their business context, e.g., *I don't think they are relevant to the business" (DB3)*. Repeatedly, the groups recalled big business attacks when asked to name recent attacks reported in the media, e.g., *"British Airways" (DD2)*. This probably reflects the paucity of news reports discussing small business attacks. Such incidents are probably deemed not newsworthy by broadcasters. However, the absence of such small business media reporting could reinforce misconceptions that cybercrime only affects large organizations. The main emotional reaction to media reporting was caution, e.g., *"It makes you want to check things" (DB6)*. This suggests that such media reports do not act as a cue to action and trigger cybersecurity adoption alone.

Table 16 shows the analysis of the cues to action sub-themes.

Very few Digitally Dependent interviewees populated cue-to-action sub-themes, suggesting they don't feel much pressure or the need to act and adopt protective security.

Table 16. Analysis of cues to action sub-themes.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Cue to action = regulatory	Cybersecurity adoption is triggered by supply chain compliance or mandatory regulation	*Compliance (DE7)*	All	30	12	27.8%
			DD	0	0	0.0%
			DB	2	2	1.9%
			DE	28	10	25.9%
Cue to action = victim	SMEs take action as a result of suffering an attack	*Predominant driver is they've been a victim (DE5)*	All	25	11	23.1%
			DD	2	2	1.9%
			DB	1	1	0.9%
			DE	22	8	20.4%
Cue to action = knowledge	Once an SME gains sufficient cyber knowledge it triggers adoption	*A decision-maker who understands the risks, tends to keep on top of it (DE3)*	All	11	9	10.2%
			DD	3	1	2.8%
			DB	3	3	2.8%
			DE	5	5	4.6%
Cue to action = est trust	Once trust is established between Digital Enabler and SME, action is more likely	*Develop a trusted partnership with an organisation (DE10)*	All	13	8	12.0%
			DD	1	1	0.9%
			DB	3	3	2.8%
			DE	9	4	8.3%
Cue to action = win business	SMEs take action if it wins business	*They can't win business unless they demonstrate that they have some basic controls in place (DE7)*	All	17	8	15.7%
			DD	1	1	0.9%
			DB	2	1	1.9%
			DE	14	6	13.0%
Cue to action = reputation	Protecting business reputation is what triggers adoption	*I do see people feeling the need to take action to protect their brand (DB10)*	All	12	5	11.1%
			DD	0	0	0.0%
			DB	11	4	10.2%
			DE	1	1	0.9%

3.20. Regulatory compliance, winning business, and being a cyber victim

Digital Enablers painted a picture that SMEs do not adopt cybersecurity proactively, believing that reactions to regulatory pressures were a significant cue to action, e.g., *"If they are part of a procurement chain, they are kind of forced into it" (DE8)*. The paucity of Digitally Dependent and Digitally Based interviewees mentioning acting to comply with regulations suggests they either operate in spaces where such regulatory pressures don't exist or are unaware of their obligations. Similarly, Digital Enablers described how SMEs acted if it meant winning business, e.g., *"If they are in the technology sector, then it will be about winning new business, you know those things come hand in glove really" (DB1)*. No Digitally Dependent and only one Digitally Based interviewee mentioned the need to adopt security to win business. This suggests they do not feel such pressures to act or are unaware of how adopting security can help them win business.

Digital Enablers strongly believed that being a victim was a significant cue to action, e.g., *"When I worked at xxxx, a big recognizable UK firm they were exposed to quite a big phishing thing at the board level. And they kept it out of the press, and they just threw a few more hundreds of thousands at getting the perimeter secure" (DB10)*. Conversely, a minority of interviewees in the other groups addressed how being victimized acted as a catalyst for adoption.

3.21. The effect of knowledge, preserving reputation and trust upon adoption

Nine interviewees felt that once sufficient cyber knowledge was gained, it acted as a tipping point and triggered adoption, e.g., *"Once I realized that there are ways of brute forcing through if you don't have a proper password, I changed mine" (DB2)*. A prominent cue to action for Digitally Based stakeholders was protecting their reputation. One Digitally Based interviewee said, *"We have to make sure our*

app is super secure because it's our brand and reputation. All of our customers are using it" (DB7). This suggests that this group was keenly attuned to the reputational damage cyber-attacks caused. The Digitally Dependent group did not link cybersecurity with brand protection. All groups agreed that if trust was established between a Digital Enabler and a client SME. It triggered adoption, e.g., *"There needs to be a good level of trust for you to actually work with a business and get them on the right path, I think" (DE1)*.

Table 17 shows the analysis of cybersecurity engagement sub-themes.

3.22. Digitally based SMEs turn to internal networks seeking word-of-mouth referrals

Our data suggest that the Digitally Based group turns to preexisting, pre-established business networks for cyber help, e.g., *"My network" (DB3)*. Digital Enablers knew of this tendency and sort to have a presence in those networks, e.g., *"We are a member of a couple of organizations, such as The North East Chamber of Commerce, and that's a good way to meet people whom we have never engaged with before" (DE3)*. It seems that the Digitally Based group wanted word-of-mouth recommendations when sourcing/evaluating cyber help, e.g., *"Normally what we've done is go*

Table 17. Analysis of cybersecurity engagement sub-themes.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Turns to business network	Digital Enablers reach SMEs by penetrating their networks. Digitally Dependent and Digitally Based groups turn to their business networks	*Local business forums (DE9)*	All	29	16	23.6%
			DD	3	2	2.4%
			DB	14	7	11.4%
			DE	12	7	9.8%
Turns to SME IT supplier	Digital Enablers reach SMEs after referral from their IT supplier. Digitally Dependent and Digitally Based turn to their existing IT supplier	*Through our developers (DB10)*	All	17	14	13.8%
			DD	5	5	4.1%
			DB	5	4	4.1%
			DE	7	5	5.7%
Too complex	Existing cyber guidance/advice is too complicated	*The complexity (DB2)*	All	15	9	12.2%
			DD	6	4	4.9%
			DB	4	3	3.3%
			DE	5	2	4.1%
Word of mouth referral	Digital Enablers reach SMEs after being recommended. Digitally Dependent and Digitally Based seek word of mouth recommendations	*Word of mouth (DE3)*	All	16	11	13.0%
			DD	1	1	0.8%
			DB	6	5	4.9%
			DE	9	5	7.3%
Guidance from CRCs**	Interviewee reports receiving cyber security guidance from Cyber Resilience Centres (CRCs)	*Newsletter and bulletins (DD6)*	DD & DB	15	9	12.2%
			DD	8	5	6.5%
			DB	7	4	5.7%
Good advice example**	Interviewee recalls an example of good advice received	*Making passwords using 3 random words (DD9)*	DD & DB	13	9	10.6%
			DD	5	4	4.1%
			DB	8	5	6.5%
Turns to Google	Digitally Dependent and Digitally Based use google to find help. Digital Enablers pay for keyword ads, ensuring favorable listings	*I'd research it on the internet (DD8)*	All	6	6	4.9%
			DD	4	4	3.3%
			DB	1	1	0.8%
			DE	1	1	0.8%
Turns to SM & marketing	Digital Enablers reach SMEs via SM/marketing. Digitally Dependent and Digitally Based find help via SM/marketing	*Through LinkedIn (DE7)*	All	5	5	4.1%
			DD	0	0	0.0%
			DB	1	1	0.8%
			DE	4	4	3.3%
Guidance from IT**	Interviewee reports receiving guidance from existing IT suppliers/web developers	*IT support will come in and suggest things (DD10)*	DD & DB	7	6	5.7%
			DD	2	2	1.6%
			DB	5	4	4.1%

**Exclusive Digitally Dependent and Digitally Based sub-theme.

through recommendation, so we've basically linked with some of our other software colleagues that we know, and we've done it through recommendation, and that's what always, generally been the starting point" (DB1). Digital Enablers echoed this and sort to be the business being referred, e.g., *"I mean referrals for any business is always the best way (DE1).*

3.23. Digitally dependent SMEs turn to google

The Digitally Dependent group's first port of call appeared to be a Google search, e.g., *"I'd resort to good old google" (DD6)*. The risk for the Digitally Dependent group is that search engine results are likely to be heavily populated by big vendors with the budget to pay for favorable search engine listings. Therefore, searching SMEs might not get the results they need, or the results are full of complex, difficult-to-understand information not pitched at their knowledge level, business maturity, and budget.

3.24. Social media and marketing

The Digitally Dependent group did not seek cyber help or guidance via social media or marketing, unlike our Digital Enabler group, which sort to reach SMEs via the same, e.g., *"We are quite heavily invested in social marketing" (DE6)*. This suggests an incongruence between Digital Enablers and the Digitally Dependent groups' social media and marketing use.

3.25. The influence of SME IT suppliers

Digitally Dependent and Digitally Based groups described how if they had a cyber need, they contact their existing IT supplier or developer, e.g., *"Probably go to my current IT provider in the first place (DD4)*. Digital Enablers were cognizant of this trend and sort to establish alliances with such SME IT suppliers, e.g., *"Via strategic partnerships with IT suppliers" (DE5)*. Digitally Dependent and Digitally Based groups described how they received cyber guidance from their IT suppliers, e.g., *"From our IT suppliers" (DB4)*.

3.26. Interviewees recalled and described good examples of cyber guidance

Regarding thoughts on existing cybersecurity guidance in circulation, there was a broad consensus that such advice was too complex, e.g., *"I received a list of things to do, but I never did anything with it as it was too complicated" (DD4)*. Interviewees described good advice as being easy to understand and actionable. The actionable element seems to be key and was summed up by a Digital Enabler who said, *"I think you know the steps already in terms of, you know, the NCSCs 10 steps of cybersecurity etc, and the general guidance is good, but I think there's a little step beyond that in terms of, this is what you need to do when it's in. From a center perspective, I guess it's hard to recommend or name products, but I think the example is missing. Okay to help yourself against phishing, do some email filtering before it even gets to you. Well, how can I do this? Well, public cloud Digital Enablers like Microsoft already do this for you. And it's just putting that last bit on the end because that's where you're almost taking them so far, and you're leaving them, yeah Otherwise, it's I have this guidance, but well, who do I turn to, and what does it actually do, that those last bits are missing" (DE5).*

Table 18 shows the analysis of Digital Enabler engagement tactics sub-themes.

3.27. Teaching SMEs about cybersecurity and using live hack demos

When we asked our Digital Enabler group what tactics they used to persuade SMEs to adopt protective security, nine out of ten interviewees told us that they took the time to teach the client, e.g., *"The first thing that's needed is often education" (DE10).* Understandably Digital Enablers used tools to help them teach, to counter inaccurate vulnerability perceptions by using live hack demos, e.g., *"You can demonstrate that you know if they are still running God forbid Windows 7 or something like that you know could potentially go into their networks, if you get the OK from them, and then you can say look I've got all this information off this machine that you thought was secure, and you know just see the cogs starting to turn. (DE10).*

Table 18. Analysis of Digital Enabler engagement tactics sub-themes.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Teaches client*	Teaching cybersecurity helps persuade SMEs to adopt cybersecurity	*Educate them (DE5)*	DE	28	9	20.4%
RA/GA*	Conducting a risk assessment/gap analysis helps persuade SMEs to adopt cybersecurity	*You've got to convince them to do a proper secuirty audit (DE3)*	DE	19	6	13.9%
Reduce Cost*	Offering free/reduced cost services persuades SMEs to adopt security	*We offer some free consultancy (DE2)*	DE	14	8	10.2%
Live hack demo*	Live hack demos help persuade SMEs to adopt cybersecurity	*Demo because there's a lack of that connection between vulnerability A and how that can be realised (DE5)*	DE	19	5	13.9%
Hard sell ineffective*	Aggressive sales tactics are ineffective when trying to persuade SMEs to adopt cybersecurity	*Never a hard sell, in terms of you need widget X (DE5)*	DE	12	5	8.8%
Refers to Gov Bodies*	Making reference to government advice helps persuade SME to adopt cybersecurity	*So that trusted voice who is echoing what has been said by companies like us (DE9)*	DE	11	5	8.0%
Fear appeals ineffective*	The use of scare tactics are ineffective e.g. trying to scare SMEs into security adoption	*Selling onfear, is something that just doesn't work (DE1)*	DE	6	5	4.4%
Reframes cybersecurity*	Puts cybersecurity into the SME business contect	*Ensure you make it relevant to meet the needs of the business (DE6)*	DE	16	4	11.7%
Tailors advice to recipient*	Tailoring the cybersecurity guidance given to the specific needs of an SME	*Depends on the stakeholder you're talking to (DE8)*	DE	7	4	5.1%
Case Study	Using cyber case studies	*Real life examples (DE9)*	DE	5	4	3.6%

*Digital Enabler group exclusive sub-themes.

3.28. Tailoring advice, conducting gap analyses/ risk assessments, keeping costs low and reframing cybersecurity

Digital Enablers sort to tailor their advice to the recipient receiving it, e.g., *"Depends on the stakeholder you're talking to" (DE8)*, as opposed to adopting a one size fits all approach. There was further evidence of bespoke approaches when Digital Enablers described how conducting risk assessments/gap analyses were a persuasive tactic, e.g., *"Doing a gap analysis, stuff like that, you know, seeing what they've got in place now, or what they haven't got in place now and you know just helping them to tick those boxes off" (DE4)*. They also sort to persuade SMEs to work with them by offering free or low-priced consultancy *"We offer some free consultancy to our clients" (DE2)*. Digital Enablers reframed cybersecurity, making it relevant to their client's context, e.g., *"Asking them what's important to them and their business, and making sure cybersecurity is applied to that context" (DE7).*

3.29. Avoid using fear appeals and hard sells

Digital Enablers told us that fear appeals were ineffective in persuading SMEs to act, e.g., *"What doesn't work is the scaremongering approach" (DE10)*. Equally, Digital Enablers held a dim view of the use of sales techniques,

Table 19. Analysis of return-on-investment (ROI) sub-themes.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
ROI = Protect Business	Interviewee states that return on investment in cybersecurity is that it protects businesses from attack	*Protects your company for the future (DB7)*	All	24	12	32.4%
			DD	9	5	12.2%
			DB	13	5	17.6%
			DE	2	2	2.7%
ROI = Reputation	Interviewee states that return on investment in cybersecurity is the protection of business reputation	*For us its reputational (DB1)*	All	12	10	16.2%
			DD	3	2	4.1%
			DB	7	6	9.5%
			DE	2	2	2.7%
ROI = Peace of Mind	Interviewee states that return on investment in cybersecurity is that it gives peace of mind	*Peace of mind (DD10)*	All	14	9	18.9%
			DD	8	5	10.8%
			DB	5	3	6.8%
			DE	1	1	1.4%
ROI = None	SMEs do not value cybersecurity/see any return on investment	*I don't see any return (DB10)*	All	20	9	27.0%
			DD	1	1	1.4%
			DB	8	4	10.8%
			DE	11	4	14.9%
ROI = Insurance	Interviewee states that return on investment in cybersecurity is that it gives them insurance	*It's protections like an insurance policy (DB3)*	All	4	4	5.4%
			DD	0	0	0.0%
			DB	4	4	5.4%
			DE	0	0	0.0%

telling us that hard sells were ineffective e.g., *"Never a hard sell in terms of you need widget X that does not work in cybersecurity" (DE5).*

3.30. Leveraging trust

Digital Enablers liked to refer to government bodies during their SME engagements, e.g., *"It makes it an easier conversation when you are pointing towards government advice" (DE1).* This suggests that Digital Enablers want to capitalize on the trust such bodies engender to reinforce their advocacy. This probably helps overcome client suspicions that they are being deceived into a sale.

Table 19 shows the analysis of return-on-investment (ROI) sub-themes.

3.31. SMEs believe there is limited return on investment in cybersecurity

Very few interviewees spoke positively about the business benefits that good cybersecurity can bring. Some interviewees were very open when they said that they felt was no return on investment in cybersecurity, e.g., "*There are no positives that come from investment" (DD5).* Digital Enablers lamented this lack of perceived return in SMEs, e.g., *"You work with a business, you identify risks and present your report, but the value of your deliverable is not fully understood and therefore is a very tough sale" (DE9).*

3.32. Giving peace of mind, protecting the businesses, reputation, and insurance

Groups discussed how implementing Cybersecurity gave them peace of mind, e.g., *"Peace of mind" (DB2).* Interviewees discussed how they felt a return was that cybersecurity protected their business, e.g., *"Protecting your business" (DD7).* The Digitally Based group felt that a return was the protection of their business reputation, e.g., *"You have a lot of it is word of mouth, and it's a relatively close-knit industry that we work in, and I think if we were to be hit by cybersecurity attack god forbid, you know information or data was stolen, or services went down, that would not reflect well on the company at all" (DE8).* This is unsurprising given that the Digitally Based group's business relies heavily on technology and data, and they are keenly attuned to how attacks could damage their reputation. The Digitally Based group linked returns on investment to insurance policies *"I just see it as insurance" (DB10)*, which suggests they recognize that they are likely to

experience an attack. In that eventuality, cybersecurity investments act as an insurance policy.

Table 20 shows the analysis of improvements that can help improve SME security adoption sub-themes.

3.33. Improve SMEs interface with existing advice

All groups felt that more cybersecurity guidance was not needed, but what needed to change was the interface or point at which recipients received advice that was already in circulation that needed to improve e.g., *"That interface with the business is as important, as the actual delivery of the content (DB5).*

3.34. Improve SME cyber awareness of threats and protective cybersecurity

All groups called for more awareness amongst the SME community, e.g., *"We could do with more education" (DB2)*. The argument here is that raising SME cyber knowledge levels will, in turn, lead to more accurate threat appraisals, as personified by one interviewee who described watching a video at a cyber awareness session on the dangers of using public Wi-Fi *"The first thing they did was said they actually got a surveillance team outside Starbucks, I think it was, and they basically showed how they used the Wi-Fi, to get people who were buying coffees details, and they wrote those details on the cups of coffee, it had all their information on the cup and I was like holy **** so I gotta do something so that on the back of that" (DD5).*

3.35. Improve advice and guidance by tailoring and simplifying it

There was agreement that guidance/advice needed tailoring to the organization receiving it, e.g., *"Ultimately what's the guidance for my size of business" (DD2)*. There was agreement that guidance/advice needed simplifying e.g., *"I'd like to have it dumbed down if that makes sense, so take out abbreviations, all the technical speak away from it, and basically do like a technical guide for idiots" (DD5),*

3.36. Digital enablers call for improvements to regulation

The only improvement sub-theme that held disagreement was the call for more regulation of the IT/cyber sector by Digital Enablers, e.g., *"Now we know the majority of SMEs aren't even following the legal requirements for this, so we need some changes to regulation or more enforcement of existing rules" (DE2)*. Only a single Digitally Dependent SME

Table 20. Analysis of improvements that can help improve SME security adoption sub-themes.

Sub-theme	Description	Illustrative Comment	Group	STC	IC	TF
Improve advice interface	Improve how existing cybersecurity guidance reaches SMEs from its source	*It's probably not about more information, cause theres plenty of it from NCSC, but its how that filters down to them that needs to change (DE6)*	All	28	17	33.7%
			DD	5	4	6.0%
			DB	12	8	14.5%
			DE	10	4	12.0%
More awareness needed	Raising the level of cybersecurity knowledge amongst SMEs	*It's just a case of more education, than anything else (DE4)*	All	13	10	15.7%
			DD	2	2	2.4%
			DB	3	2	3.6%
			DE	8	6	9.6%
Tailor cyber guidance	Tailor cybersecurity guidance to the individual business receiving it, as opposed to a one size fits all approach	*They need tailored consultancy to improve (DE7)*	All	16	10	19.3%
			DD	4	4	4.8%
			DB	7	4	8.4%
			DE	5	2	6.0%
Simplify cyber guidance	Simplify existing cybersecurity guidance, making it suitable for the lay person	*Simplify it (DD9)*	All	15	8	18.1%
			DD	9	4	10.8%
			DB	4	2	4.8%
			DE	2	2	2.4%
More regulation required	Calls for changes to existing regulation or more regulation of the cybersecurity/IT sector	*Lots of companies say they do cybersecurity but they all do it differently (DE1)*	All	11	7	13.3%
			DD	1	1	1.2%
			DB	0	0	0.0%
			DE	10	6	12.0%

discussed regulatory improvements. It's possible that many of our Digitally Dependent and Digitally Based interviewees lack the necessary knowledge and understanding of the sector's initial regulations, hindering their ability to suggest or comprehend the need for regulatory improvements.

4. Discussion

Our qualitative interviews have yielded a rich dataset that offers insights across five key areas:

- ***Risk Perception in SMEs***: Factors Influencing Cyber Risk Judgments and Perceptions.
- ***Protective Cybersecurity***: Defensive Measures, Security Knowledge, Adoption Barriers, the Role of SME IT Suppliers and the Cybersecurity Sector.
- ***SME Perspectives on Cybersecurity***: Cues to Action and Return on Investment.
- ***SME Cybersecurity Engagement***: Help-seeking, Support Networks, Advice, and Effective Strategies.
- ***Enhancing SME Cybersecurity Adoption***: Exploring Future Improvements.

In the following discussion, we will expand upon our understanding of those areas with reference to the academic literature, after which we identify this study's limitations, future work, recommendations, and conclusions.

Risk Perception in SMEs considers subthemes related to SMEs' perception of vulnerability to cyber-attacks, their views on hacking, and the impact of business cyber-attack news reporting. By gaining deeper insights into how SMEs assess risk and understanding the factors that influence their assessments, we can develop targeted interventions to address and rectify inaccurate risk perceptions. Such interventions are essential for enhancing SMEs' cybersecurity posture and promoting effective risk management practices.

4.1. Risk perception: It won't happen to me

According to statistical analysis, a comparison between Digitally Dependent, Digitally Based groups and Digital Enablers' perceptions of cyber-attack vulnerability showed significant variations. Digitally Dependent SMEs tended to perceive their vulnerability as low, or they expressed uncertainty about their level of vulnerability. Digitally Based SMEs described their vulnerability as low or average, while Digital Enablers believed that most SMEs were highly susceptible to cyber-attacks. Consistent with prior research (Osborn et al., 2017; Renaud & Weir, 2016; Wilson et al., 2022), our study revealed that SMEs generally do not believe their business is at risk of a cyber-attack. Previous studies have demonstrated that SMEs have difficulty measuring cyber risk (Alahmari & Duncan, 2020; Osborn et al., 2017; Van Haastrecht et al., 2021). Our findings contribute to this understanding by revealing that the Digitally Dependent, Digitally Based, and Digital Enablers groups hold differing perceptions of vulnerability. Therefore, SMEs require personalized support when evaluating cyber risk. Both the Digitally Dependent and Digitally Based groups mistakenly believed that their small size would make them less attractive to hackers, relying on security through obscurity, an observation repeatedly made by our Digital Enablers.

Additionally, there was a discrepancy in the group's perceptions of the most threatening types of cyber-attacks. The Digitally Dependent and Digitally Based groups were primarily concerned about targeted attacks, whereas the Digital Enablers thought untargeted/opportunistic attacks presented the greatest risk. These findings align with previous studies, indicating that SMEs generally lack sufficient knowledge of cyber threats and hacker motivations (Hoppe et al., 2021; Osborn et al., 2017). This knowledge gap highlights the need to educate about the dangers of opportunistic attacks, emphasizing hacker tactics, goals, and motivations among less tech-savvy SMEs. Prior research by Osborn et al. (2017) highlighted how their participants, with high levels of IT knowledge, were concerned about the risks posed to SMEs by opportunistic attacks. This further underscores the importance of addressing this specific knowledge gap in groups with low-security knowledge. According to the Microsoft Digital Defence Report (2022), there has been a global increase in targeted and opportunistic attacks that share

similar methodologies. For instance, a company with inadequate external infrastructure security can be vulnerable to both automated and human-operated attacks, regardless of whether they are targeted or opportunistic. Thus, it is crucial to raise awareness among Digitally Dependent and Digitally Based SMEs regarding the essential security measures they must implement to mitigate most opportunistic attacks (Such et al., 2019). Support and guidance are necessary for SMEs to understand how these measures protect their business effectively. A survey by Wilson et al. (2022) found that SMEs are aware of the business impacts cyber-attacks pose, yet they perceive their likelihood of attack as low. This further highlights the importance of providing SMEs with the necessary support to assess risks effectively.

4.2. Risk perception: views on hacking and hackers

Our research found that Digitally Dependent SMEs had an exclusive belief that hackers primarily target their banking and personally identifiable information (PII), overlooking the diverse range of cyber-attacks and attack vectors. They need to understand the opportunistic nature of cyber-attacks, where the theft or compromise of generic data is often the main objective for attackers rather than specifically targeting their data or business (Seralathan et al., 2018). Open-source threat reports (Microsoft, 2022; Verizon, 2021) describe phishing attacks' prevalence on businesses. It is, therefore, not surprising that all our groups discussed phishing attacks and described how they felt vulnerable to such attacks.

The Digitally Dependent and Digitally Based groups harbored stereotypical notions about hackers wearing hoodies, and a few interviewees associated hacking with organized crime. When asked about hackers, half of our study's Digitally Dependent and Digitally Based groups provided a stereotypical portrayal. In their assessment of cybersecurity awareness campaigns, Bada et al. (2015) observed that most campaigns featured images of hackers sitting in front of computer screens. They argued that such images were typically fear appeals and text recommending protective measures to mitigate the threat. However, the literature has conflicting views on the effectiveness of fear appeals in changing cybersecurity behavior (Renaud & Dupuis, 2019). The pervasive use of hooded hacker imagery may not evoke fear or resonate with the intended audience (Bada et al., 2015), potentially reinforcing misconceptions that all hackers are teenage bedroom operators and unlikely to target small businesses. This may further promote the misconception of security through obscurity. The Microsoft Digital Defence Report (2022) states there are numerous threat actors with varying skills and motives, and hooded figure imagery does not accurately reflect the diversity of the threat nor resonate with SMEs (Bada et al., 2015). In contrast, more Digitally Based participants in our study associated hackers and hacking with organized crime, which is a more accurate depiction of the threat landscape (Microsoft, 2022). This may be because this group had a better understanding of the threats. Our findings suggest that greater awareness of hackers and their connections to international organized crime is necessary, and awareness campaigns should avoid using stereotypical hooded imagery.

4.3. Risk perception: the influence of cyber-attack news reporting

Our findings suggest that SMEs' perceptions of cyber-attack reporting in the news are closely related to their perceptions of cybercriminals. The Digitally Dependent and Digitally Based groups believed such reporting was irrelevant to their business context, and news of attacks on big businesses only triggered concern but not action. In line with this, a survey by Wilson and McDonald (2023) found that media reporting of cyber-attacks on businesses did not trigger action among SMEs. In contrast, Wolf et al. (2021) found disagreement among small business chief information security officers (CISOs) regarding the influence of media reporting, with some feeling it would trigger action, others feeling it would not, and some viewing such reports as sensationalized. Our interviews with Digital Enablers revealed similar disagreement regarding the influence of news stories. Based on

their experience, some Enablers believed such stories reinforced the misconception that cyber-attacks exclusively target large businesses. Conversely, other Enablers thought these stories would increase SMEs' attention and motivate them to act. We suggest convincing Digital Enablers to either articulate the relevance of such news stories to small businesses and demonstrate their susceptibility to such attacks or to refrain from mentioning them altogether.

Protective Cybersecurity encompasses various sub-themes that shed light on the security implemented by SMEs, the barriers they encounter in resource allocation, the influence of IT suppliers, and the overall impact of the cybersecurity sector on SMEs. By gaining a comprehensive understanding of the diverse perspectives within different SME groups regarding what constitutes effective cybersecurity and the factors shaping those perspectives, we can provide enhanced support to SMEs in implementing robust protective security measures.

4.4. Protective cybersecurity: tech-centric approaches

Our findings report that SMEs lack a comprehensive understanding of cybersecurity measures, consistent with prior research that suggests they focus on easily implementable technical solutions and typically adopt a tech-centric approach to cybersecurity (Osborn et al., 2017)., It is also widely reported that SMEs lack sufficient cybersecurity training (Wilson et al., 2022) and policies/processes (Hoppe et al., 2021). To promote effective cybersecurity, best practice frameworks such as ISO27001 emphasize balancing the three pillars of people, processes, and technology (Schneier, 2009). Organizations should ensure that all three pillars are equally important and maintain a harmonious relationship. Our study found that the Digitally Dependent Group was more inclined to adopt a tech-centric approach than the Digitally Based Group, which operates in a more technical environment and likely has a greater understanding of the benefits of people and process-based approaches. Digitally Dependent and Digitally Based SMEs should aim to increase their knowledge and appreciation of the value of a balanced approach to people, processes, and technology to enhance their cybersecurity posture. One area of focus is logging, with none of the Digitally Dependent and only two Digitally Based interviewees indicating that they scrutinized their logs for any suspicious activities. As one Digital Enabler described, *"You'll get a breach, and then it's like, oh, you know what's happened? Well, nobody knows because you not logging anything" (DE1)*. This corresponds with previous SME studies, which have also identified deficiencies in logging and monitoring practices (Kreppein et al., 2021). Effective logging practices enable a retrospective analysis of incidents, and proactive monitoring can identify signs of known attacks or unusual system behavior (NCSC, 2021).

4.5. Protective cybersecurity: resource barriers

Consistent with previous studies (Alahmari & Duncan, 2020; Eybers & Mvundla, 2022), our findings indicate that financial constraints, time limitations, and a lack of expertise are common barriers to SMEs' adoption of cybersecurity measures. However, we noticed that the issue of financial constraints appeared to be less concerning for the Digitally Dependent group than the Digitally Based and Digital Enabler groups. It is possible that they have not sought quotes for security consultancy and are unaware of the potential costs, or their business nature and size make their security needs less expensive than those operating in a more technical space. We confirm previous findings that SMEs prioritize other business functions over cybersecurity (Eybers & Mvundla, 2022). When SMEs claim that they lack the time or money for cybersecurity or have more pressing demands, it may be because they do not fully comprehend the relevance of cybersecurity to their business. As a result, they do not allocate resources, which leads to prioritization of other business functions. The Digital Enabler group provided useful insights into addressing such perceptions by framing cybersecurity in the business context, making it more relevant to the recipient.

4.6. Protective cybersecurity: the influence of SME IT suppliers

The Digitally Dependent and Digitally Based groups highlighted their existing IT supplier as

one of their primary resources for addressing cybersecurity concerns or issues. Recognizing the importance of this relationship, the Digital Enablers actively pursued strategic alliances with SME IT suppliers to engage with SMEs effectively. This aligns with Renaud and Weir (2016), who concluded that local IT companies played a critical role in SME cybersecurity based on their survey of 110 Scottish SMEs. However, our Digital Enablers expressed concerns about the competency of SME IT suppliers, as they observed that many lacked the necessary cyber knowledge and skills to assist SMEs with their cybersecurity needs effectively. Cartwright et al. (2023) interviews with thirteen SME IT suppliers/cyber consultants revealed that IT companies can positively and negatively impact SME cybersecurity. They argued that interventions are required to enhance SME security, such as guiding micro and small businesses in selecting reliable IT companies and offering support to IT suppliers lacking cybersecurity expertise. Surprisingly, neither the Digitally Dependent nor Digitally Based groups expressed concerns about the cyber competency of their IT suppliers. However, McLaurin (2021) survey of SME owners or managers highlighted that SMEs lack the knowledge to assess the capabilities of their IT suppliers. This is concerning because our data suggest that the Digitally Dependent and Digitally Based groups believe their IT suppliers ensure their protection against cyberattacks. This presents a twofold risk: firstly, IT suppliers may lack the necessary cyber expertise and provide inadequate advice, and secondly, they may focus solely on defensive technological measures, lacking the experience and knowledge to implement training and policies. This observation partially explains the tech-centric approach evident in our data.

To demonstrate competency in technical cybersecurity, cyber consultancies can obtain a range of security accreditations (NCSC, 2023a). However, these certifications can be costly for consultancies to obtain, making their services too expensive and a barrier for price-sensitive SMEs. Moreover, these certifications are often more suited to large organizations' needs and risk profiles, not SMEs. IT suppliers face a difficult situation when clients ask for cybersecurity help. If they admit a lack of knowledge/expertise, they risk losing their clients' confidence and potentially losing them to competitors. National CRC Centers (2023) offer an opportunity to address these concerns by providing security assessments that suggest mitigation routes rather than supplying IT to SMEs. In situations where cyber queries are beyond their expertise, IT suppliers could refer SMEs to CRCs with confidence that they will not lose the customer to the CRC. While research on the role of IT suppliers in SME cybersecurity is limited, our study contributes to the existing knowledge in this area. We suggest that efforts be made to improve IT suppliers' cybersecurity knowledge and harness their influence with SMEs to promote good cybersecurity practices.

4.7. Protective cybersecurity: the influence of the cybersecurity sector

All groups perceived that the cybersecurity industry was excessively sales-driven, which can result in a reluctance to engage. This finding is consistent with previous research identifying similar concerns among SME managers (Watad et al., 2018). Digital Enablers believed that vendors sometimes prioritized sales over the efficacy/suitability of their product for SMEs, potentially misleading them into a false sense of security. This finding was also reported in previous research (Osborn et al., 2017). Interestingly, none of our Digitally Dependent or Digitally Based interviewees mentioned this behavior, suggesting they are unaware of the potential for such unethical practices. To counter such unethical practices, a two-pronged approach is necessary. Firstly, sector regulation with appropriate penalties and enforcement could deter unethical practices. Our Digital Enablers called for such regulation when asked what could be done to improve the future of SME cybersecurity adoption. However, raising awareness and understanding of existing regulations is necessary, as SMEs often don't understand the legislation and are unaware of how it relates to their business and what action to take to comply (Hoppe et al., 2021). Therefore, even if new legislation were to be created, it might not have the desired effect without accompanying awareness campaigns and relevant support. Secondly, it could be helpful to raise SME awareness of the potential to be misled and provide

them with a list of trusted cybersecurity companies that will not use unethical practices. To address this issue, the UK's trusted authority, the NCSC, has created a list of approved companies that offer SME-centric consultancy, primarily based on implementing cyber essentials technical controls (NCSC, 2023b). However, the NCSC may not be able to set the costs of such consultancy, as the marketplace determines the prices. With a shortage of cyber skills and the cost of cyber accreditations, the price may be too high a barrier for most SMEs.

Cybersecurity Perspectives include the sub-themes that explore various factors that influence SMEs' decisions regarding cybersecurity adoption. The factors include mandatory compliance, experiencing cyber-attacks, cyber knowledge, trust, winning business, reputation protection, and return on investment. By examining these triggers, we can gain valuable insights into the mind-set of SMEs and devise effective strategies to promote cybersecurity awareness and engagement.

4.8. Cybersecurity perspectives: cues to action

Digital Enablers said that the primary trigger for SMEs to adopt cybersecurity measures was mandatory compliance within supply chains or enforced regulation. This is consistent with Wolf et al. (2021) findings. However, our Digitally Dependent and Digitally Based groups did not mention such compliance. It is possible that they have not yet encountered such regulations or do not consider them applicable to their business. Similarly, Digital Enablers described that an SME experiencing a cyber-attack was a significant driver for security adoption (Wolf et al., 2021). Only a small number of Digitally Dependent and Digitally Based interviewees reported being victims of online crime in our pre-interview screening survey, which could partially explain the lack of Digitally Dependent and Digitally Based groups mentioning this trigger, as those who have not experienced an incident may not have had to re-evaluate their security. Alternatively, our screening data could be skewed, with some respondents hesitant to reveal being victims of an attack due to adverse reputational impacts. Digitally Based and Digital Enabler groups believed that sufficient cyber knowledge would trigger SME decision-makers to take protective action, a finding consistent with other literature (Saban et al., 2021). However, only one Digitally Dependent interviewee mentioned this trigger, which indicates a lack of cyber knowledge in this group.

All groups said trust was a trigger, with clients being more likely to act if they trusted a cyber provider. Digital Enablers often refer to trusted sources of cybersecurity advice, such as the UK government and the National Cybersecurity Center (NCSC), to leverage trust. Heidt et al. (2019) interviews with twenty-five SME IT experts also found that trust was important for SME engagement. However, Osborn et al. (2017) interviews with SME IT users revealed that a lack of trust in the cyber sector due to unethical sales practices could hinder security adoption. This highlights the issue of trusting the wrong people, as one Digitally Dependent interviewee described how they were more likely to act on advice from someone they trusted, even if it was wrong. Furthermore, it could be difficult for outsiders (those who are yet to earn trust) to intervene and counteract advice from a trusted business yet impart incorrect cyber advice to an SME. Therefore, engaging with SME IT suppliers to improve SME cybersecurity is crucial, as they will likely have an established, trusted relationship that could be harnessed.

According to the Digital Enabler group, adopting cybersecurity measures would be more likely if it led to winning business. Kosutic (2021) interviews with security officers, executives, consultants, and IT managers found that investing in cybersecurity can increase a business's competitive advantage, supported by other research (Barlette et al., 2017). SMEs may be more willing to act on cybersecurity if they perceive that their customers demand it or want to keep up with their competitors investing in security measures. However, our Digitally Dependent and Digitally Based groups seemed less motivated by this trigger, suggesting they either do not feel the need to act to win business or have not yet faced such situations. Digital Enablers deliberately reframe and reposition cybersecurity to persuade SMEs to invest in

cybersecurity to win more business. Research has shown that investing in cybersecurity can increase the value of a business (ISC2, 2018), and we suggest emphasizing this point during SME encounters.

Our Digitally Based group consistently emphasized the importance of safeguarding their reputation, which served as a trigger for action. This is not surprising given the technical nature of their business; a security breach could significantly harm their reputation, leading to a loss of customers. Other researchers (Osborn et al., 2017; Wolf et al., 2021), who interviewed IT providers and SME CISOs, also found that protecting reputation was a strong motivator. Interestingly, our pre-interview survey revealed that most Digitally Dependent and Digitally Based interviewees processed personally identifiable information (PII), which has a legal requirement to be adequately protected (ICO, 2023). Failure to do so can result in fines, data processing bans, and negative publicity. Despite this, no Digitally Dependent interviewees discussed the impact of failing to protect PII on their reputation. This suggests that this group may need additional support to understand their obligations under the law, the importance of safeguarding PII data, and the consequences for their reputation.

4.9. Cybersecurity perspectives: return-on-investment

There is a lack of research on how different SME categories might perceive return on investment differently. Protecting a business's reputation from the adverse impacts of an attack was the Digitally Based group's primary motivator and perceived return. The same group likened cybersecurity to insurance, suggesting they felt some protective benefit from implementing defensive measures. However, the intangibility of cybersecurity makes it challenging to quantify returns, as some authors have noted (Haney & Lutters, 2018; Heidt et al., 2019). Some interviewees from Digitally Dependent and Digitally Based groups felt that there was limited return on cybersecurity investment. Digital Enablers expressed frustration at the perceived lack of value SMEs placed on cybersecurity. Nonetheless, research has shown that investment in cybersecurity can increase a business's value and competitive advantage (ISC2, 2018; Kosutic, 2021). The cybersecurity industry tends to focus on fear appeals, such as data breaches, fines, and business disruptions, which can be insufficient in changing behavior (Ahluwalia, 2000). Lloyd (2020) argues that cybersecurity advantages such as improved revenue, profit, and growth from effective cybersecurity measures are seldom highlighted. SME awareness strategies and engagement practices need to emphasize the positive aspects of cybersecurity rather than defaulting to fear appeals.

Cybersecurity Engagement encompasses various sub-themes vital for understanding how SMEs seek cyber help, identify sources to turn to when facing security issues, perceive existing cybersecurity advice and guidance, and evaluate the effectiveness of engagement strategies. Examining these sub-themes provides valuable insights into SMEs' challenges in navigating the cybersecurity landscape.

4.10. Cybersecurity engagement: a lack of awareness of government initiatives

Previous studies (Renaud & Ophoff, 2021; Renaud & Weir, 2016) have shown that SMEs have limited engagement with government websites or information related to cybersecurity. Similarly, our research on awareness of the UK's National Cybersecurity Center (NCSC) indicates that the Digitally Based group has much greater awareness of the center, while the Digitally Dependent group does not. This highlights the need to improve the Digitally Dependent group's awareness of such initiatives, especially in light of findings showing that acting upon NCSC advice can significantly improve SMEs' cybersecurity (Such et al., 2015).

4.11. Cybersecurity engagement: how do SMEs source cybersecurity help?

Digitally Based SMEs typically sourced any cybersecurity requirements internally, relying on their existing business networks and seeking recommendations through word-of-mouth rather than seeking

solutions outside their network. Few Digitally Dependent SMEs reported doing the same. This suggests that Digitally Dependent SMEs have not formed networks containing technical knowledge. While previous research on small business relationships found that SMEs tend to go "internal" rather than "external" when seeking help (Street & Cameron, 2007), inward-looking behavior could be counterproductive as internal networks may not contain the required cyber expertise (Heidt et al., 2019). Digital Enablers proactively established a presence in SME business networks by engaging with groups, such as the chambers of commerce, to reach SMEs effectively. Building relationships and establishing trust in such small business networks could be an effective strategy for reaching SMEs.

Our research also revealed that word-of-mouth referrals dictated whom the Digitally Based group turned to for cyber help, while few Digitally Dependent SMEs used this approach. Instead, Digitally Dependent SMEs turned to Google searches for security, a finding confirmed in other SME survey-based research (Renaud & Weir, 2016). However, search engine results may not return the help and information tailored to their needs, as they are likely to be populated by vendors with the financial resources to pay for and dominate favorable listings, selling solutions tailored to big business. The sub-theme of sourcing cyber help and guidance via social media and marketing was closely related to internet searching for security. Only one Digitally Based interviewee tried to source help via social media and marketing channels, while four Digital Enablers actively used these channels to reach SMEs. This disparity means that time, effort, and money could be wasted trying to reach Digitally Dependent and Digitally Based SMEs or proffering help and guidance via such methods. Wolf et al. (2021) interviews with small business CISOs found that cyber marketing could be unhelpful to SMEs, as there was too much of it, and SMEs did not know where to start. Instead, SME marketing campaigns should be simple, tailored, actionable, and provide some post-action feedback (Bada et al., 2015)., All our groups complained that existing cyber guidance/advice was too complex, a finding echoed in the literature (Renaud & Weir, 2016), meaning those who design such campaigns must react accordingly. However, relying solely on marketing to impart cybersecurity advice could be less effective as no trust or prior relationship with the intended audience has been established. Finally, all groups unanimously agreed that the distribution of existing advice to SMEs needed to improve. This corresponds to findings from previous research (Renaud & Ophoff, 2021).

4.12. Cybersecurity engagement: ineffective strategies

Digital Enablers felt that using hard sells or fear appeals was ineffective and sometimes even counterproductive when engaging SMEs in cybersecurity, and a few of our Digitally Dependent and Digitally Based interviewees echoed this. This aligns with previous research indicating that using fear appeals with small businesses may not yield the desired results (Bada et al., 2015). However, Haney and Lutters (2018) study showed that some cybersecurity advocates used small doses of fear to help SMEs understand risk. However, crucially, they provided solutions to mitigate those risks and ease anxiety. While using fear appeals remains a topic for further investigation, our Digital Enablers felt fear could hinder SME security adoption.

Future improvements in SME cybersecurity adoption encompass various sub-themes that explore actionable steps to enhance security practices. These sub-themes delve into strategies to increase awareness, promote education and training, refine guidance delivery, and advocate for regulatory changes. Organizations and policymakers can work toward bolstering SME cybersecurity and mitigating potential risks by addressing these areas.

Digitally Dependent and Digitally Based groups said they needed to improve their security knowledge. Digital Enablers highlighted that their primary method of promoting cybersecurity adoption among SMEs was to teach SMEs about cybersecurity so that they understood enough to know why it was necessary and how it related to them. This finding corresponds with recommendations from previous studies (Eybers & Mvundla, 2022; Haney & Lutters, 2018; Luuk et al., 2023). Digital Enablers used teaching aids such as tailored risk assessments, identifying specific protective actions, and using live hacking demos to show how easily their business could

be hacked without basic security controls. Haney and Lutters (2018) found similar risk assessment approaches used by security advocates they interviewed. Digital Enablers also tailored their advice and guidance to the context and knowledge levels of the recipient. This is consistent with previous recommendations to move away from a one-size-fits-all approach and tailor cybersecurity guidance to the intended recipients' (Heidt et al., 2019; Tam et al., 2021; Wolf et al., 2021). Some researchers suggest that a specific SME security advocate role should be created and fulfilled by those who know how to bridge the gap between security experts and non-experts (Haney & Lutters, 2018). Such advocates will use techniques like tailoring and a better understanding human behavior to communicate cybersecurity advice effectively.

All groups believed improving the interface of how current advice reaches SMEs was important. However, this did not mean increasing the volume of guidance but ensuring that more of the existing guidance reaches SMEs. Digital Enablers called for regulatory changes to establish what constitutes effective SME cybersecurity and to prevent some IT companies from overstating their expertise. In contrast few Digitally Dependent and Digitally Based groups called for any regulatory changes. This indicates they may be unaware of existing regulations, or the danger posed by some SME IT suppliers who lack the required cybersecurity skills and knowledge to be competent.

4.13. Recommendations

Table 21 contains this study's recommendations for improving SME cybersecurity.

Table 22 presents the most prevalent cyberattacks affecting UK businesses and recommended ISO-aligned mitigations involving People, Processes, and Technology.

4.14. Limitations, future work, and reflections on approach

This study has a few limitations. Firstly, a more diverse sample across micro, small, and medium-sized SMEs would have been preferable. However, obtaining thirty complete interviews is noteworthy, considering previous research highlighting the challenges in recruiting SMEs for such studies (Osborn et al., 2017; Tam et al., 2021). It is important to acknowledge the potential influence of bias in our findings. Most of our interviewees were affiliated with Cyber Resilience Centers (CRCs). This association could introduce a positive bias, as interviewees may feel inclined to express favorable views regarding CRCs. Nevertheless, given the difficulties in recruiting SMEs for research, this approach was pragmatic. A concern with interviews is the potential for self-report bias. Participants may alter their responses to present themselves in a favorable light, particularly as the first author is a serving police officer. This decision was deliberate as the officer could leverage his connections with small businesses to recruit willing SME participants and overcome the risk of inadequate recruitment. Furthermore, participants may be more inclined to trust a serving officer and, consequently, be more truthful. When interviewees discuss defensive measures to safeguard their businesses, we cannot ascertain whether they are appropriately configured and effective. The secondary coding of our entire data set was impossible due to resource constraints. The authors, therefore, calculated ICR based on secondary coding of at least 25% of the interviews. This approach followed observations that 10–25% of secondary coding was typical (O'Connor & Joffe, 2020). While data from UK small businesses can provide valuable insights into the challenges faced by global small businesses, it's essential to recognize potential differences across other global regions that may exist. Considering the broader global context is crucial, as variations in regulatory environments and cultural norms could influence small business cybersecurity perspectives and engagement preferences.

To expand on this study, future research could involve interviews with IT suppliers who work with SMEs. This could provide valuable insights into how to engage with suppliers to enhance SME cybersecurity effectively. Additionally, if a consensus could be reached on defining start-up businesses, similar studies could be conducted to understand their unique user needs and compare them with those of Digitally Dependent and Digitally Based SMEs.

Table 21. Recommendations and strategies to improve future SME cybersecurity adoption.

Call to action	Recommendations	Benefiting Group
Improve how existing cybersecurity guidance reaches SMEs	Harness SME IT suppliers' influence and trust with SMEs to disseminate cybersecurity advice and guidance to promote protective measures	DD & DB
	Harness the influence of local business clubs and small business networks to disseminate advice and guidance	DD & DB
	Consider utilizing favorable Google search engine listings to guide SMEs toward existing government advice websites.	DD
Counter the potential lack of cyber knowledge/ expertise that might exist in some SME IT suppliers	Increase SME awareness of the difference between IT and cybersecurity and the potential limitations of suppliers	DD & DB
	Educate IT suppliers on the benefits of training people and implementing sound business processes for SMEs' security, countering tech-centric approaches	DD & DB
	To prevent potential embarrassment and alleviate concerns about losing SME clients, IT suppliers refer SMEs to CRCs when they are operating outside their area of cyber expertise	DD & DB
	To address the issue of individuals falsely claiming to be SME cyber experts, it is important to explore regulatory changes that establish clear qualifications and experience requirements for legitimate experts in this field.	DD, DB & DE
	Refer SMEs to the NCSCs approved list of SME cyber vendors	DD & DB
Improve SME knowledge of cyber threats	Educate SMEs about the risks associated with untargeted, opportunistic cyber-attacks	DD & DB
	Challenge the misconception that SMEs have nothing worth stealing or are too small to be attacked.	DD & DB
	Exercise caution when referring to news reports of cyber-attacks on large businesses to avoid misleading SMEs into thinking that such incidents are irrelevant or that attackers exclusively target larger companies.	DD & DB
	Avoid perpetuating stereotypes of hackers wearing hoodies, which do not accurately reflect the organized nature of cybercrime.	DD & DB
	Educate on the goals, aspirations, and methodology of attackers, countering the notion that they are primarily targeting PII and want to steal back details	DD
	Counter inaccurate risk appraisals by conducting live hacking demonstrations when appropriate, highlighting the ease with which businesses can be hacked.	DD & DB
Improve SME knowledge of protective cybersecurity	Increase awareness about the importance of cybersecurity training and policies for both people and processes. It is crucial for SMEs to recognize that relying solely on technical protective measures is insufficient. They need to understand how training and policies can effectively safeguard their business.	DD & DB
	Highlight the importance of security monitoring and logging to detect suspicious activity.	DD & DB
	Simplify cybersecurity guidance and avoid technical jargon to ensure it is accessible to non-technical audiences.	DD & DB
	Tailor guidance to the knowledge level of SMEs to increase comprehension and successful implementation.	DD & DB
	Make guidance actionable by providing clear, specific steps for implementation.	DD & DB
	Reframe and reposition cybersecurity guidance to align with an SME's specific business context	DD & DB
Improve SME Cybersecurity Engagement	To enhance visibility and benefit from word-of-mouth recommendations, individuals or organizations seeking to improve security for SMEs should actively participate in SME networks	DE
	To foster trust with SMEs, individuals or organizations aiming to enhance security should prioritize building, maintaining, and improving relationships. Referring to trusted sources of advice, such as government agencies, can help in this regard.	DE
	Harness reputational cues as a means to motivate certain SMEs who prioritize their brand	DB
	Utilize positive language to encourage adoption: Instead of employing fear appeals, reframe cybersecurity in a positive context and emphasize the benefits of investment to foster greater adoption.	DE
Overcome resource barriers to cybersecurity adoption	To address the price sensitivity of SMEs, it is crucial to minimize security costs, perhaps by providing flexible payment options that allow SMEs to spread payments for cybersecurity	DE
	Enhance awareness of cybersecurity funding sources, such as grants or vouchers provided by local enterprise partnerships, to help subsidize costs for SMEs.	DE
	Refer SMEs to Cyber Resilience Centers (CRCs) [60] for heavily subsidized cybersecurity consultancy services on a not-for-profit basis. Alternatively, direct SMEs to the UK police cyber protect network [60] for free expertise and guidance.	DD & DB
	Reframe the significance of cybersecurity for SMEs by using effective engagement tactics that educate them on its relevance and the impact it has on their business.	DD, DB & DE

Table 22. Top 3 Cyber-attacks on UK Businesses in the 2023 Cybersecurity Breaches Survey, Along with Key People, Processes, and Technological Mitigations.

Attack Type	Description	Approach to Mitigation
Phishing	Deceptive e-mails designed to trick recipients into disclosing sensitive information or performing harmful actions, such as clicking on links or opening attachments.	**Technological**: E-mail filtering (SPAM) to detect and stop malicious e-mails from reaching users. Detection of malicious URLs to prevent users from accessing harmful websites after clicking on links, leveraging the most effective strategies validated by recent research in this field (Waseso & Setiyanto, 2023). Automatic scanning of attachments to identify and quarantine malicious files. **People**: Staff training on how to spot malicious e-mails and what action to take should one be encountered. **Processes**: Reporting mechanisms for employees to report suspected phishing e-mail attempts.
Organizational E-mail Impersonation	E-mails that impersonate legitimate organizations to deceive recipients into making fraudulent payments	**Technological**: Implement e-mail authentication protocols like SPF, DKIM, and DMARC to detect and prevent e-mail spoofing. Utilizing machine learning and artificial intelligence (AI) to identify and prevent potentially fraudulent payments (Ojugo et al., 2023). **People**: Employee training on recognizing signs of e-mail impersonation. **Processes**: Verifying e-mail sender identities through additional means (e.g., phone call)
Malware	Malicious software designed to infiltrate systems, steal data, or cause harm.	**Technological**: Installation and regular updates of reputable antivirus and antimalware software. Implementation of software updates and patch management to address vulnerabilities. Secure configuration of systems and networks to reduce attack surface. **People**: Employee training in safe practices, emphasizing the importance of avoiding the use of unfamiliar or untrusted removable media like USB sticks. **Processes**: Regular backups of critical data to mitigate the impact of malware infections.

Reflecting on the overall approach using Digital Enablers as proxies to understand the cybersecurity views and engagement preferences of Digitally Dependent and Digital Based SMEs is an innovative approach. It offers researchers a broader reach that traditional recruitment methods cannot achieve due to Digital Enablers' extensive exposure to SMEs. This cascade effect enables researchers to industrialize their reach. This is significant because SMEs are reluctant to engage directly with researchers. However, they do engage to some extent with Digital Enablers. Using Digital Enabler as proxies, researchers effectively overcame the SME engagement barrier, providing this study with valuable perspectives and insights. Drawing from the literature and the Health Belief Model (HBM), the authors created a discussion guide to shape the focus of interviews. The HBM provided a useful theoretical framework for initial areas of questioning, allowing flexibility to explore unexpected and intriguing responses. It is important to clarify that the authors did not aim to test or validate the HBM in relation to SME attitudes and behaviors but used it as a source of inspiration for their questions. Alternatively, the Protection Motivation Theory (PMT), which shares similar constructs with the HBM, could have been considered a suitable alternative theory to guide interview questions in this study.

5. Conclusions

In summary, SME cybersecurity is not a one-size-fits-all proposition. It requires a tailored approach due to different groups' unique characteristics and perspectives. Our study revealed variations in risk perceptions, resource barriers, knowledge levels, and engagement preferences among the groups. Particularly, the differences between Digital Enablers and the Digitally Dependent/Digitally Based groups were more pronounced than the disparities between the Digitally Dependent and Digitally Based groups. Notable distinctions emerged in areas such as the perceived targets of hackers, the importance placed

on safeguarding reputation, the significance of word-of-mouth referrals, and the perspective on cybersecurity as a form of insurance for Digitally Dependent groups. Conversely, Digital Enablers exhibited disparities in their perception of opportunistic attacks as the greatest risk to SMEs, the recognition of compliance as a primary motivator for adopting digital solutions, the importance of securing new business opportunities through cybersecurity measures, and their call for increased regulations. Furthermore, Digital Enablers identified small business IT providers as potential barriers to effective SME cybersecurity. These findings highlight the need for tailored interventions and support to address different SME groups' specific challenges in their cybersecurity endeavors.

Acknowledgments

We thank the anonymous reviewers for their valuable feedback and the NEBRC and CRC network for their assistance during the research. We would also like to sincerely thank the SMEs and cybersecurity providers who generously contributed their time and insights to our study.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Martin Wilson http://orcid.org/0000-0001-8886-6527
Sharon McDonald http://orcid.org/0000-0002-4774-634X

Data availability statement

The participants of this study did not give written consent for their data to be shared publicly, so due to the sensitive nature of the research, supporting data is unavailable.

References

Abraham, C., & Sheeran, P. (2015). The health belief model. In M. Conner, & P. Norman (Eds.), *Predicting and changing health behaviour: research and practice with social cognition models* (3rd ed., pp. 30–55). Open University Press.

Ahluwalia, R. (2000). Examination of psychological processes underlying resistance to persuasion. *Journal of Consumer Research*, *27*(2), 217–232. https://doi.org/10.1086/314321

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1–5). https://doi.org/10.1109/CyberSA49311.2020.9139638

Almeida, F., Carvalho, I., & Cruz, F. (2018). Structure and challenges of a security policy on small and medium enterprises. *KSII Transactions on Internet and Information Systems (TIIS)*, *12*(2), 747–763. https://doi.org/10.3837/tiis.2018.02.012

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). *Cyber security awareness campaigns: Why do they fail to change behaviour?* 118–131. https://doi.org/10.48550/arXiv.1901.02672

Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter? *Systèmes d'information & management*, *22*(3), 7. https://doi.org/10.3917/sim.173.0007

Berisha, G. (2015). Defining small and medium enterprises: A critical review. *Academic Journal of Business, Administration, Law and Social Sciences*, *1*(1), 17–28.

Bernard, H. R. (2017). *Research methods in anthropology: Qualitative and quantitative approaches*. Rowman & Littlefield.

Cartwright, A., Cartwright, E., & Edun, E. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of it companies. *Computers & Security*, 103288. https://doi.org/10.1016/j.cose.2023.103288

Dieye, R., Bounfour, A., Ozaygen, A., & Kammoun, N. (2020). Estimates of the macroeconomic costs of cyber-attacks. *Risk Management and Insurance Review*, *23*(2), 183–208. https://doi.org/10.1111/rmir.12151

DSIT. (2023, April 19). *Cybersecurity breaches survey 2023*. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

Engels, C., Francis, B., & Philip, D. (2022). The cost of privacy failures: evidence from bank depositors' reactions to breaches. *Available at SSRN 3625668*. https://doi.org/10.2139/ssrn.3625668

Eybers, S., & Mvundla, Z. (2022). Investigating Cyber Security Awareness (CSA) amongst managers in small and medium enterprises (SMEs). In T. Antipova (Ed.), *Comprehensible Science* (Vol. 315, pp. 180–191). Springer International Publishing. https://doi.org/10.1007/978-3-030-85799-8_16

Friese, S. (2019). *Qualitative data analysis with ATLAS. ti*. Sage.

Haney, J. M., & Lutters, W. G. (2018). "It's scary ... it's confusing ... it's dull": how cybersecurity advocates overcome negative perceptions of security. *Proceedings of the 14th Symposium On Usable Privacy and Security (SOUPS)*, June 2018 (pp. 411–425).

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational it security investments. *Information Systems Frontiers*, *21*(6), 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: Insights from industry surveys. *The Journal of Risk Finance*, *22*(3/4), 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Hutton, G. (2022). *Business statisitcs*. House of Commons Library Business Statisitcs. https://researchbriefings.files.parliament.uk/documents/SN06152/SN06152.pdf

ICO. (2023). *Guide to the UK General Data Protection Regulation (UK GDPR)*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

ISC2. (2018). *Cybersecurity assessments in mergers and acquisitions. The ROI Of Sound Cybersecurity Programs*. https://www.isc2.org/-/media/ISC2/Research/The-ROI-of-Sound-Cybersecurit-Programs/MAcybersecuritySurveyReportvF92019.ashx

Kergroach, S., & Bianchini, M. (2021). *The Digital Transformation of SMEs*. OECD Publishing. http://www.sela.org/media/3222564/the-digital-transformation-of-smes.pdf

Kosutic, D. (2021). *The impact of cybersecurity on competitive advantage* [Student thesis]. Grenoble ecole de management]. https://www.researchgate.net/profile/Dejan-Kosutic-2/publication/357826918_The_Impact_of_Cybersecurity_on_Competitive_Advantage/links/61e143d270db8b034c92052e/The-Impact-of-Cybersecurity-on-Competitive-Advantage.pdf

Kreppein, A., Kies, A., & Schmitt, R. H. (2021). Novel maturity model for cybersecurity evaluation in industry 4.0. *Advances in Cyber Security*, *1487*, 198–210. https://doi.org/10.1007/978-981-16-8059-5_12

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security*, *2015*(3), 5–7. https://doi.org/10.1016/S1361-3723(15)30017-8

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud & Security*, *2020*(2), 14–17. https://doi.org/10.1016/S1361-3723(20)30019-1

Luuk, B., Susanne V 't H de, G., Ellen, M. H., Ynze, H. H., Remco, S., & Eric Rutger, L. (2023). Protecting your business against Ransomware Attacks? Explaining the Motivations of Entrepreneurs to Take future Protective Measures against cybercrimes using an extended protection motivation theory Model. *Computers & Security*, 103099. Published onlinehttps://doi.org/10.1016/j.cose.2023.103099

Madani, A. E. (2018). SME policy: Comparative analysis of SME definitions. *The International Journal of Academic Research in Business & Social Sciences*, *8*(8), 103–114. https://doi.org/10.6007/IJARBSS/v8-i8/4443

McLaurin, T. (2021). *A study on the efficacy of small business cybersecurity controls* [Student thesis]. Marymount University]. https://www.proquest.com/openview/1b62edd74dae78b5c6f70ed7f4708071/1?pq-origsite=gscholar&cbl=18750&diss=y

Microsoft. (2022). *Microsoft digital defence report 2022*. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

National CRC Group. (2023). Regional Centres—National CRC Group. https://nationalcrcgroup.co.uk/regional-centres/

NCSC. (2018). *Regional Organised Crime Units (ROCUs)*. https://www.ncsc.gov.uk/search

NCSC. (2020). *Small Business Guide: Cyber Security*. https://www.ncsc.gov.uk/collection/small-business-guide

NCSC. (2021). *10 Steps to cyber security. Logging and monitoring*. https://www.ncsc.gov.uk/collection/10-steps/logging-and-monitoring

NCSC. (2023a). *CHECK - Penetration Testing*. https://www.ncsc.gov.uk/information/check-penetration-testing

NCSC. (2023b). *Cyber Advisor*. Cyber Advisor. https://www.ncsc.gov.uk/schemes/cyber-advisor

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

O'Connor, C., & Joffe, H. (2020). Intercoder reliability in qualitative research: Debates and practical guidelines. *International Journal of Qualitative Methods*, *19*, 1–13. https://doi.org/10.1177/1609406919899220

Ojugo, A., Maureen, A., Ejeh, P., Ashioba, N., Odiakaose, C., Ako, R., & Emordi, F. (2023). Forging a user-trust hybrid memetic modular neural network card fraud detection ensemble: A Pilot study. *Journal of Computing Theories and Applications*, *1*, 1–11. https://doi.org/10.33633/jcta.v1i2.9259

Osborn, E., Simpson, A., & Osborn & Simpson. (2017). Risk and the small-scale cyber security decision making dialogue—A UK case study. *The Computer Journal*, *61*(4), 472–495. https://doi.org/10.1093/comjnl/bxx093

Pagura, I. (2020). Small business and cyber security. *Journal of the Australian Traditional-Medicine Society*, *26*(1), 38–39. https://search.informit.org/doi/10.3316/INFORMIT.070004091643509

Parkin, S., Fielder, A., & Ashby, A. (2016). Pragmatic security: Modelling it security management responsibilities for SME archetypes. *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats* (pp. 69–80). https://doi.org/10.1145/2995959.2995967

Renaud, K., & Dupuis, M. (2019). Should we scare people into behaving securely? *Network Security*, *2019*(11), 20. https://doi.org/10.1016/S1353-4858(19)30135-7

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 24–46. https://doi.org/10.1108/OCJ-03-2021-0004

Renaud, K., & Weir, G. R. S. (2016). Cybersecurity and the unbearability of uncertainty. *2016 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 137–143). https://doi.org/10.1109/CCC.2016.29

Reynolds, T. J., & Gutman, J. (1988). Laddering theory, method, analysis, and interpretation. *Journal of Advertising Research*, *28*(1), 11–31. http://www.dl.edi-info.

ir/Laddering%20theoy,%20method,%20analysis,%20and%20interpretation.pdf

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude Change1. *The Journal of Psychology*, *91* (1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, Y., Sharp, H., & Preece, J. (2023). *Interaction design: Beyond human-computer interaction*. John Wiley & Sons.

Saban, K. A., Rau, S., & Wood, C. A. (2021). "SME executives' perceptions and the information security preparedness model". *Information & Computer Security*, *29*(2), 263–282. https://doi.org/10.1108/ICS-01-2020-0014

SBS. (2020). *The EU cybersecurity act and the role of standards for SMEs—position paper*. European DIGITAL SME Alliance Brussels. https://www.sbs-sme.eu/sites/default/files/publications/23032020%20SBS%20Position%20Paper_EU%20Cybersecurity%20Act%20and%20the%20role%20of%20standards%20for%20SMEs.pdf ,

Schneier, B. (2009). *Schneier on security*. John Wiley & Sons.

Seralathan, Y., Oh, T. T., Jadhav, S., Myers, J., Jeong, J. P., Kim, Y. H., & Kim, J. N. (2018). *IoT security vulnerability: A case study of a web camera*. 172–177. https://doi.org/10.23919/ICACT.2018.8323686

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for approaching cybersecurity competence and awareness. *The 16th International Conference on Availability, Reliability and Security* (pp. 1–7). https://doi.org/10.1145/3465481.3469200

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research techniques*. Sage publications.

Street, C. T., & Cameron, A.-F. (2007). External relationships and the small business: A review of small business alliance and network research. *Journal of Small Business Management*, *45*(2), 239–266. https://doi.org/10.1111/j.1540-627X.2007.00211.x

Such, J. M., Ciholas, P., Rashid, A., Vidler, J., & seabrook, t. (2019). basic Cyber Hygiene: Does it work? *Computer*, *52* (4), 21–31. https://doi.org/10.1109/MC.2018.2888766

Such, J. M., Vidler, J., Seabrook, T., & Rashid, A. (2015). *Cyber security controls effectiveness: a qualitative assessment of cyber essentials*. http://www.research.lancs.ac.uk/portal/en/publications/cyber-security-controls-effectiveness(a09a2d28-d121-41dc-86d6-cc24595d8968)/export.html

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses. *Computers & Security*, *109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

Tebb, K. P., Erenrich, R. K., Jasik, C. B., Berna, M. S., Lester, J. C., & Ozer, E. M. (2016). Use of theory in computer-based interventions to reduce alcohol use among adolescents and young adults: A systematic review. *BMC Public Health*, *16*(1), 1–33. https://doi.org/10.1186/s12889-016-3183-x

Van Haastrecht, M., Yigit Ozkan, B., Brinkhuis, M., & Spruit, M. (2021). Respite for SMEs: A systematic review of socio-technical cybersecurity metrics. *Applied Sciences*, *11*(15), 6909. https://doi.org/10.3390/app11156909

Verizon. (2021). *2021 Data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/

Waseso, B., & Setiyanto, N. (2023). Web phishing classification using combined machine learning methods. *Journal of Computing Theories and Applications*, *1*, 11–18. https://doi.org/10.33633/jcta.v1i1.8898

Watad, M., Washah, S., & Perez, C. (2018). It security threats and challenges for small firms: Managers' perceptions. *International Journal of the Academic Business World*, *12* (1), 23–30. https://www.jwpress.com/Journals/IJABW/BackIssues/IJABW-Spring-2018.pdf#page=29

Whitehead, G. (2020). *Investigation of factors influencing cybersecurity decision making in Irish sme's from a senior manager/owner perspective* [Student thesis]. National College of Ireland]. https://norma.ncirl.ie/4804/1/gerardwhitehead.pdf

Wilson, M., & McDonald, S. (2023). SME cybersecurity misconceptions: A guide for decision-makers. In N. Vajjhala & K. Strang (Eds.), *Cybersecurity for Decision Makers* (pp. 293–316). CRC Press.

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2022). It won't happen to me: Surveying SME attitudes to cybersecurity. *Journal of Computer Information Systems*, *63*(2), 397–409. https://doi.org/10.1080/08874417.2022.2067791

Wolf, F., Aviv, A. J., & Kuber, R. (2021). Security obstacles and motivations for small businesses from a {CISO's} perspective. *30th USENIX Security Symposium (USENIX Security 21)* (pp. 1199–1216). https://www.usenix.org/conference/usenixsecurity21/presentation/wolf